

3 1761 11648461 9

Digitized by the Internet Archive
in 2023 with funding from
University of Toronto



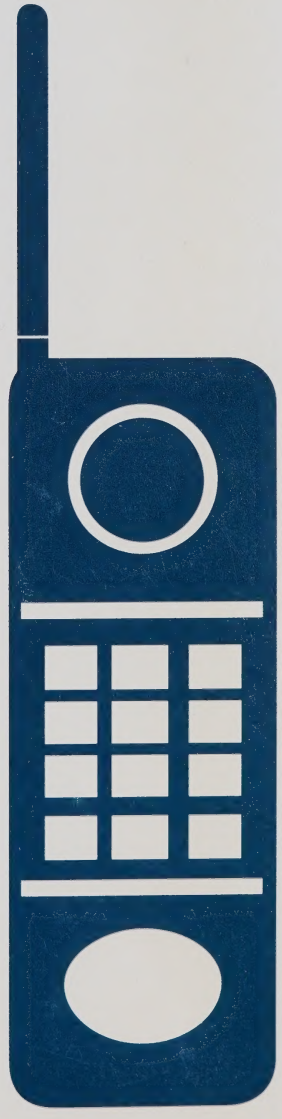
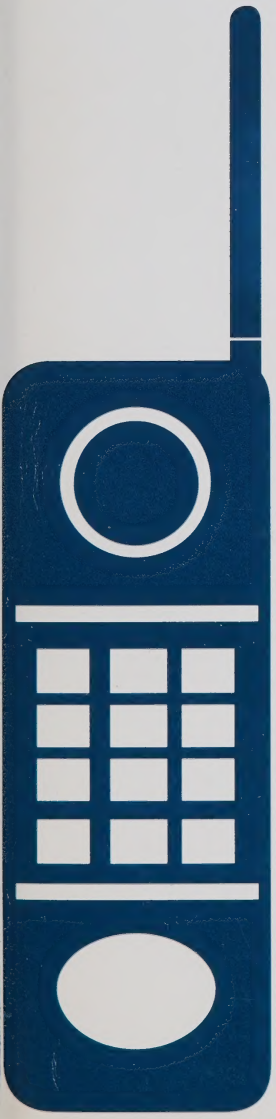
CAI
PC
-AST

112

Government
Publications

Privacy Commissioner

Annual Report 1992 - 1993



Annual Report Privacy Commissioner 1992-93

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa



June 30, 1993

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report.

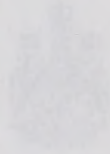
This report covers the period from April 1, 1992 to March 31, 1993.

The Privacy Commissioner of Canada
115 Kent Street
Ottawa, Ontario
K1A 1H5
Tel: (613) 993-1200
Fax: (613) 993-1207
TDD: (613) 993-1207

© Canada Communication Group
Cat. No. IP-93-11982
ISSN 0-522-5040-7

This publication is available in audio cassette.

Annual Report
Privacy Commissioner
1992-93



The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-2410, 1-800-267-0441
Fax (613) 995-1501
TDD (613) 992-9190

© Canada Communication Group
Cat. No. IP 30-1/1993
ISBN 0-662-59840-7

This publication is available on audio cassette.

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

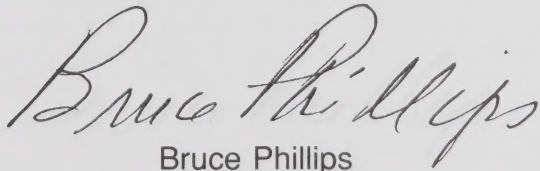
June 30, 1993

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1992 to
March 31, 1993.

Yours sincerely,

A handwritten signature in cursive script that reads "Bruce Phillips". The signature is written in dark ink and is positioned above the printed name and title.

Bruce Phillips
Privacy Commissioner

The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa


June 30, 1993

Dear Mr. Fraser:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1992 to
March 31, 1993.

Yours sincerely,

A handwritten signature in cursive script that reads "Bruce Phillips".

Bruce Phillips
Privacy Commissioner

Mandate

The Privacy Commissioner is a specialist ombudsman—appointed by and accountable to Parliament—who monitors the federal government's collection, use and disclosure of its clients' and employees' personal information, and its handling of individuals' requests to see their records.

The *Privacy Act* gives the Commissioner broad powers to investigate individuals' complaints, to launch his own complaint, and to audit 160-odd federal agencies' compliance with the *Act*. He also conducts research on his own behalf or at the request of the minister of justice.

Mission

The Privacy Commissioner's mission is

- to be an effective ombudsman's office, providing thorough and timely complaint investigations to ensure Canadians enjoy the rights set out in the *Privacy Act*;
 - to be an effective privacy guardian on Parliament's behalf, performing professional assessments of the quality of the government's adherence to the *Privacy Act*;
 - to be Parliament's window on privacy issues, arming it with the facts needed to make informed judgements through research and communications;
 - to be the primary national resource centre for research, education and information on privacy.
-

Table of Contents

Ten Years After	1
Rising to the Technology Challenge	
Delivering service electronically	13
A privacy checklist	14
Other works in progress	16
Privacy on the Hill	
Protecting cellular calls	19
Telecom privacy principles	20
Amending the <i>Income Tax Act</i>	22
Privacy in Banking	25
...On the Streets	
<i>Privacy Revealed: the Canadian privacy study</i>	27
...In the Courts	
Privacy Commissioner vs. Canada Post	29
SINs for birth registration	30
Patient access to medical records	31
...In the Labs	
Biotechnology update	32
...Here and There	
In the provinces	37
Overseas	39
...In the Private Sector	
The CSA model Code	43
CDMA privacy code	44
...In the Office	
Investigating Complaints	45
How institutions measured up	45
Notifying the Commissioner	48
Inquiries	54

Table of Contents

Some cases	57
Tables and charts	70
...In the Office	
Assessing Compliance	75
Special investigations	75
Institution audits	77
Following up	81
It's 1993—Do you know where your information is? . .	85
Corporate Management	90
Organization Chart	92

Ten years after

Publication of this report falls on the tenth anniversary of the coming into force of the federal *Privacy Act* and with it the creation of the Office of the Privacy Commissioner. The question naturally posed by such an occasion, of course, is whether the birthday is a happy one.

Let us acknowledge the truth that any anniversary which the subject is still around to observe has something going for it. And certainly the progeny shows signs of promise. All the same, we're disinclined to break out the cake and champagne.

Call the mood one of subdued satisfaction. The office is gratified at having given ten years of useful service helping Canadians exercise their privacy rights in their relations with the Government of Canada. That service includes more than 7,500 investigations completed and findings rendered, almost 25,000 inquiries received and answered, and major audits of about one-third of the government's information holdings conducted—no small achievement for an office which has never held as many as three dozen persons.

Despite the sceptics' direst predictions, law enforcement has not ground to a halt, there has been no sweeping abandonment of honest record-keeping and departments have not found themselves repeatedly before the courts. Nor have individuals' requests to examine their personal information yet brought any department to its knees (although until it changed its policy, privacy applications had National Defence reeling).

In fact, the *Act*, the complaints and audits have prompted many government institutions to better identify, organize and fine-tune their record-keeping—no small benefit in an era when virtually all government agencies have converted to electronic information systems.

And this Office can lay some claim to stimulating public debate about data matching, control of the Social Insurance Number, the

privacy implications of biotechnology, privacy principles in telecommunications services, controls on cellular telephone eavesdropping, privacy regulations in the financial sector and entrenching privacy rights in the *Charter*.

Many of these initiatives demonstrate graphically the changing role of this tiny office. Mandated (and funded) only to investigate complaints against 160-odd federal institutions, the Commissioner is under pressure from Parliamentarians, the public and media to answer their privacy questions, to comment on the privacy implications of new programs and legislation, to appear before committees, and to speak out on the issues beyond his narrow mandate. To refuse is to court irrelevancy. To accede is to risk insolvency. Parliament's privacy ombudsman strives to meet the demands but the budget is reaching crisis point.

However, the climate of fiscal restraint has far broader privacy implications. Pressured to rationalize programs, improve service and cut costs, the government is aggressively pursuing ways of conducting much of its business electronically. Direct deposit of benefit cheques is just the beginning. Already the federal government is using electronic data interchange (EDI) to collect GST and personal income tax, to document immigrants and refugees and collect customs duties at the borders.

One proposed new system is an interactive network of government information kiosks ("Infocentres") which will allow clients to get information about government services, check job openings, apply for various programs and send change-of-address notices to participating departments. Once in place, the network can be substantially expanded to become a one-stop shopping centre for federal government services.

These new electronic systems make a qualitative change to government information handling, including three ominous characteristics. The first is the need to have an identification card to receive the services, implying personal identification numbers,

probably photographs and, quite possibly, fingerprints or some other biometric identifier.

The second is the likely private sector involvement in any electronic interchanges of personal data—a sector without any legislated privacy controls.

Finally, the costs of developing and delivering these new services could demand government consolidate its programs across departments—and perhaps even across federal-provincial jurisdictions. The walls between databases may come tumbling down, raising once again the spectre of the single government file—or profile—and the spectre of Big Brother.

There is no shortage of work for a privacy commissioner.

In a “technological trance”

Any remaining temptation to celebrate is more than offset by an acutely painful awareness that increasingly we know only enough to realize how little we know. The office spends a good deal of time fighting fires. And in the wider world beyond the federal government and the limited reach of the *Privacy Act*, birthday celebrations may be premature.

Viewed in that wider context, several developments in the past decade have effectively laid siege to privacy:

- the explosion of computer technology, leaping from powerful mainframes, to personal computers, to electronic notebooks—each step bringing smaller, more mobile, more powerful and more accessible tools capable of being linked around the world, and the increasing sophistication of computer software;
- Western societies’ uncritical acceptance of technology—including no systematic consideration of its impact

on individual rights. We are in what has been described as a “technological trance”—technology drives individuals’ rights rather than the other way around and the response, both in the private and public sectors, has been sporadic, tentative, and only marginally effective;

- the rapid evolvement of biotechnology from a tool aimed at improving human health, to a powerful commercial and political weapon with an ominous potential for social surveillance and control;
- the “commodification” of information—the packaging of information as a commercial good which in an increasingly competitive business environment is seen as lighting the path to economic competitiveness.

And threats to informational privacy are only one part of the global privacy problem. Growing encroachments on physical privacy and increased physical surveillance round out the dilemma. Although perhaps beyond the general focus of this report on privacy of information, they form crucial elements of the chemistry of intrusion.

How long will it be before calls for better crime prevention put cameras at major street corners in our urban areas? In the name of suppressing crime, Canadians may see their own lawful movements monitored by the state. Perhaps Orwell was not wrong.

And the increasing use of technology to monitor workers is another omen. With each new form of surveillance we become less like individuals and more like automatons, monitored for defects and aberrant behaviour that will consign us to the reject pile or mark us for “corrective” measures.

Some experts feel that the game is already over, that technology has laid bare the life stories of us all, that Canadians should

consign the concept of individual control to history, stop worrying and learn to live with and love the free flow of information.

Privacy revealed

Thankfully, public awareness of the impact of technology on privacy has also grown during the past decade. One useful development was the release in the Spring of 1993 of the first major national study of public attitudes on privacy issues. The study provides the first hard statistical evidence that Canadians are alive to the privacy issue—incontrovertible proof if any were needed that privacy is not some elitist concern or fringe issue. The fact that 52 percent of the population voices “extreme concern” with the state of personal privacy ought to satisfy the most sceptical lawmaker or regulator. There is a strong public consensus on giving privacy a higher priority on the policy agenda.

This survey, sponsored and financed by a consortium of private and public sector organizations (including this Office) also revealed that Canadians know what they need to protect their privacy in an information society. An overwhelming majority said they want some control over the gathering of information about them; to be told in advance when it’s being collected, by whom and for what purpose, and to have the right to consent to or refuse any transaction involving information about them. In short, they want those things that are the foundation of fair information practices, and which are absent from so much of today’s traffic in personal data.

The Canadian public has thus grasped the essence of the privacy issue in the information age—personal control over the information which others know or can learn about them. The survey reveals a widespread sense of uneasiness; 61 per cent **strongly** agreed that “consumers have lost all control over how personal information about them is circulated and used by companies.” And 60 per cent agreed that they have less privacy in their daily lives than they did ten years ago. Those whose business is studying

this matter know only too well how justified Canadians are in harbouring that belief.

Canadians are familiar with some highly-publicized privacy disasters including those resulting from monitoring and disclosure of cellular telephone conversations. But, in all probability, this is decidedly minor-league compared with the personal information about them that is routinely exchanged over computerized data bases and easily available to persons whose right to the information is, at best, debatable.

Thanks to numerous congressional investigations, and a fairly aggressive media community, a considerable body of knowledge has developed in the United States detailing the scope and nature of information trafficking through computerized data bases. Horror stories abound. For example, in one of the latest works, *Privacy For Sale*, author Jeffrey Rothfeder (himself not a computer expert) relates how, with little difficulty, he gained access to the credit reports of former U.S. Vice-President Dan Quayle and television anchorman Dan Rather.

He also recounts how every resident of a small New England town was listed as a tax evader by a credit reporting company, thanks to a computer input error. None of the 1,500 persons knew about this damning but inaccurate information until one of them, an affluent physician (presumably unused to being denied credit) looked into the matter.

Given the similarity in Canadian and U.S. business practices one must assume the very real possibility of similar events taking place in Canada. Just to cite a few recent examples culled from the media:

- a grocery chain began issuing “smart cards” to provide discounts to customers but neglected to tell them that their spending habits would be profiled and sold to direct marketing companies;

-
- a company given sensitive medical files to destroy, sold the documents to a television production company where they were used on camera as props;
 - eight employees of a credit reporter misrepresented themselves as Revenue Canada employees to trace customers owing money to a provincial utility;
 - a chartered bank released clients' card numbers, names, addresses and other personal data to a market research firm to test demand for new products;
 - a man checking the accuracy of his credit file found several inquiries about him from a lawyer in a province where he has no business or personal contacts. He has no legal recourse because there is no national credit reporting legislation and no privacy protection in the private sector;

No-one reading any of these stories can rest easily.

Leaving a “datashadow”

Ten years ago, the first annual report of this office observed:

...it has become trite to say that personal privacy is threatened as never before in human history...The confluence of new technologies with ever-insistent claims of the state to know, to be efficient, or both, has changed the qualitative and quantitative nature of the problem.

If the threat was so well understood and clearly visualized 10 years ago, what does it say about the situation today? It says that, with limited exceptions, the situation is decidedly worse. Everybody is acquainted with the enormous increase in direct marketing, for instance—the floods of advertising mail, the nightly phone calls. While these are nuisances (and some would argue, easily dealt with) they depend on access to highly-detailed

personal profiles of customer prospects. Yet how many of us know what is in those profiles, or where the information came from, or who has them, or how accurate they are, or how secure they are, or, what is worse, to whom they might be sold? Not many.

The fact is, ten year's technology has transformed the inherent value of personal information. Every scrap of data about us, from such mundane "tombstone" information as name and age, to lifestyle data such as shopping habits or movie preferences, to such detailed medical information as our genetic makeup, is useful to somebody. Technology has furnished us with the tools to buy, manipulate, re-constitute and sell the details of others' lives for a profit. Under the harsh glare of all this electronic scrutiny Canadians leave a "datashadow"—a trail of personal details and transactions which they cannot control.

Consider the privacy implications of just two new technological developments: powerful new national information networks and the new personal communication devices. The first, the Canadian Network for the Advancement of Research Industry and Education (CANARIE) is a national initiative to stimulate creation of a high-speed digital network by the year 2000. The network will use optical fibres to connect the public and private sectors and citizens coast to coast. The federal government alone has earmarked millions of dollars over the next five years for the project. In five years, the amount of data being transmitted over electronic networks will grow 2000-fold. In effect, networks like these will transform information flow in the same way the transcontinental railroad did the flow of people and goods a century ago, and as modern highway networks did in this century.

The optical superhighway will revolutionize communication, carrying on its hair-thin glass fibres not just the words in electronic messages and computerized medical records but even such images as X-rays and Electrocardiograms.

The next five years will bring yet another new telecommunication tool; personal communications networks. These networks will redefine how Canadians use the telephone. Numbers will be assigned, not to locations, but to individuals. Calls will be routed through radio transmitters, satellites and computers, tracking down the recipient and feeding the communication. And the new devices will be capable of handling voice, audio, text and graphic display.

Useful as these devices may be, there are looming privacy problems. Not only is the content of the call at risk—this is wireless communication after all—but the more insidious invasion is the potential for surveillance. One has only to place a call and the telephone company will know (and the billing records will show) where both caller and recipient were, and when. Will these records be available to government? To police? Will they be sold for marketing purposes?

Facing the music

Must we continue to argue about the desperate need to get a better handle on the business of information? Trailing far behind in the information race is any effort to produce some reasonable respect for the rights of the individuals whose personal information is the raw material for this industry. The ten years since the first privacy commissioner drew attention to the “threat” have seen the gap between problem and solution yawn ever wider.

Frankly, it is becoming tiresome to hear people with a vested interest in unfettered information flow exclaim how “difficult” it is to protect privacy, when one suspects what they really mean is how “inconvenient.”

One cannot fail to observe how readily solutions are found when specific cases force their way onto the public agenda. The recent example of intercepted cellular telephone calls leaps to mind. Once some sensitive political disclosures thrust the vulnerability of

these devices on politicians and the public, the legislative machinery was remarkably quick to propose a remedy.

So the evidence that solutions exist is recent and graphic. What is needed now is the will to deal with the issue in more than piecemeal fashion. One lesson the past ten years has taught: the pace of technological change makes unworkable proposing technical fixes for each new tool. We cannot envisage where technology will lead. What is needed is a privacy framework—a set of principles against which the new products and services can be measured.

These observations in no way denigrate or diminish the value of much useful work now being done. On the contrary, the last annual report and this one draw attention to encouraging developments. Indeed there has been commendable action on several fronts which we report later. But the time has come for a more aggressive and co-ordinated approach to the problem of reconciling privacy protection with the informatics revolution.

Canadians are entitled to respect for their privacy no matter what government jurisdiction, no matter what industry sector, and no matter what technology. The Commissioner pressed strongly during the recent constitutional debate for entrenching in the *Charter* an explicit right to privacy. But there were other priorities. Nevertheless, it is imperative to develop a set of principles to secure those rights. These principles should include:

All governments should recognize that every Canadian is entitled to the data protection rights expressed in such documents as the OECD privacy protection guidelines and the federal *Privacy Act*.

Broadly speaking, this means that personal information should be collected only when truly warranted, used only for the purposes set out beforehand, disclosed only in narrowly defined circumstances and accessible to the individual it concerns,

including the right to ask for correction. And the mere words in codes or statutes are not enough. Governments must be willing to establish a means of ensuring compliance with these tenets.

All governments should recognize that such privacy rights should apply to public and private sector alike.

Where such rights do not exist, the obligation rests with government to secure them.

All Canadians are entitled to be fully informed about the potential impact of technology on their lives—what information is involved, what will be done with it—and how to regulate the use of technology.

A commitment of this kind necessarily implies greatly improved public education. It also requires coordinated federal and provincial efforts to marshal the expertise capable of understanding and explaining the implications of technology on personal privacy. An equivalent to the U.S. Office of Technology Assessment might be a good starting point. The OTA helps legislative policymakers anticipate and plan for the consequences of technological change, and examine how technology affects people's lives.

The objective now should be to strengthen and extend the protection. Obviously, where more than one jurisdiction is involved, there must be leadership. It seems equally obvious that the government of Canada is best positioned to provide it. The Commissioner recommends that Parliament take steps to develop a national action plan aimed at achieving the objectives set forth in the proposed principles.

The issue, remember, is not whether technology will continue to change our lives. It will. The issue is whether the changes will be governed solely by what the technology itself makes possible, without regard to the consequences for timeless and deeply-held values such as respect for individual autonomy and privacy.

All technology, from the invention of gunpowder to nuclear fission, has had the capacity to serve ends both ill and benevolent. The computer is no different. The decision, as always, is ours to make. But we no longer have the luxury of time—the next ten years could tell the tale.

Rising to the technology challenge

Delivering services electronically

The next decade will challenge all governments to be more accessible to their taxpayers; to provide information, services and benefits directly to the individual—all at a time of eroding resources. The federal government's strategy to meet this challenge is to enhance its services by innovative use of interactive technologies.

Given the range of programs and services the government delivers, the issues are complex and the investment costs enormous. And new technological advances often threaten to undermine individual control of personal information and to erode the protection offered by privacy laws.

The federal government has recognized that, until now, technology and the technologists have operated in isolation to drive personal information management. But that is about to change. Government now acknowledges that technology simply offers us choices and that human values—including privacy—must be a part of developing and applying new information systems.

To begin with, the government has created an electronic services initiative secretariat within Treasury Board to develop a coordinated vision and framework for introducing new electronic services. The secretariat will help departments use technology as their primary means of renewing services, determine what services can be delivered electronically and provide guidance on how best to implement that technology.

Recognizing this Office's ongoing concern and interest in the issue, Treasury Board has invited the Commissioner to work in partnership, providing advice on protecting personal information in the development of new electronic services and communication systems.

The invitation (gratefully accepted) recognizes the legitimate place for privacy in the debate. Reasonable privacy protection is not incompatible with technological change; there simply must be a convergence of disciplines that will build human values into the design and application of new systems.

The Office also hopes to work with government officials to establish an interdepartmental working group on privacy and technology.

As a first step, the Commissioner has proposed a “privacy checklist” to guide senior government officials during the design stage. While the search for a “framework” goes on, the proposal would at least ensure respect for clients’ and employees’ privacy. What follows is an informal sketch of some of the issues that need to be considered.

A Privacy Checklist

Openness/Transparency: Individuals must be thoroughly informed of their rights under the new technologies. Before introducing new systems, government must notify the public about the development, its objectives and extent, the type of data to be collected and used and the individuals who will be affected. Those individuals should also be given specific notice of their right to refuse to participate; to know what information is involved in the technological process; and to be made aware of the situations likely to develop around the use of the technology.

Informed Consent: Individuals must be informed clearly and their consent obtained for all uses and disclosures of the information being processed. Individuals should also have the right to withdraw consent for uses or disclosures without penalty.

Gate Keeping: Security measures must prevent misuse or inadvertent access to individuals’ data. This means incorporating

a combination of personal identification numbers (PINs) with internal security mechanisms for individual transactions.

Matching: Systems shared by several users should be segregated internally to prevent possible merging or cross-over of personal information during any transaction. All transactions must be secure to and from the host computer.

Access: Individuals must have the right of access to and correction of the information held about them as a result of any transaction.

Non-Discrimination: New technologies must not limit the government services offered to a client and services offered electronically must respect the universality of government programs. (However, it is evident that even when participation is voluntary, participants may enjoy such advantages as faster service or service after normal business hours.)

Beneficence: Government must acknowledge and affirm that new technologies are tools to help deliver service to individuals—**not** instruments to enable it to exert control over individuals' information. (Of course, there are exceptions for the legally-mandated authority of government to properly control and administer its programs.) Government must resist the temptation to use any technology to conduct overt and covert surveillance on its citizens.

Respect: All intermediaries must respect the principles of privacy ethics or laws—all participants in the process must be made aware of and adhere to those principles.

Responsibility: Those entering information into systems must exercise the highest standard of responsibility to ensure the reliability of the system.

The checklist may strike some as a tall order—it may mean additional steps. But the privacy agenda can be incorporated into the technological arena in a way that will ensure taxpayers both improved government service and enhanced privacy protection.

Other works in progress—smart cards

This privacy checklist is drawn largely from *A Privacy and Smart Card Framework*, prepared by this Office as part of a users guide for the federal working group on implementing smart card technology. The paper sets out both an ethical framework for using smart cards as well as standards and guidelines that will take privacy protection into account in the applications design of smart card systems.

The working group is attempting to identify the possible government applications for smart card technology and to suggest an operational framework in which the cards would function.

The Department of Communications (after an earlier and unsatisfactory brush with the technology in its infancy in 1988) has begun several pilot projects. These include using the cards to control inventory of expensive high tech equipment at its Communications Research Centre and to replace the in/out employee board at the Canadian Conservation Institute. DOC also plans to use smart cards as electronic “money” in its stockrooms. The card will be loaded with an amount and each purchase will be deducted from the balance and the transactions recorded electronically.

DOC is also considering using smart cards to store employees’ passwords for access to various computer systems. Employees will have to remember only their personal identification number which will give them access to their various system passwords. The passwords will be protected by the card’s encryption capabilities.

Given the cards' ability to validate identity, employment status and security clearance, the most likely government-wide application of the technology is an employee card. The challenge will be to ensure it does not become a tracking device. However, the Office is convinced that government can devise standards and guidelines that will harness the technology, improve program delivery and still respect individual privacy.

Telework

The smart card group is just one of a number of committees on which privacy staff are working. Another is the Telework project committee. This committee will assess the results of a three-year pilot project to allow some employees to work at home and send the product to the employer electronically.

The government has recognized that information technology can help us deal with wider social issues such as allowing employees to achieve a better balance between their work and personal lives, as well as reducing energy consumption and pollution and easing traffic congestion.

The government has also acknowledged that while working at home can be beneficial, it also has some privacy implications. How will government protect clients' (and other employees') personal information while it is off the premises or in transit? And how will it ensure that working at home does not compromise employees' private home life?

Security safeguards for personal data must equal those provided at the work site. How much security will depend on the sensitivity of the personal information and the protection provided by each government agency. Clearly some agencies will allow teleworking with personal data; others will not.

The committee will examine the results of the project and its implications (not just for privacy). Its report is expected in late 1995.

Public Service Compensation System

The Office will also review the new public service compensation project, a huge single database to store the pay and benefit information of all federal employees and pensioners. The implications of a single database are substantial; linking and merging of data, movement of data between departments, need for security safeguards and restricting access to those who need to know. The challenge will be to ensure that this system does not become the single, all-inclusive government profile.

Privacy on the Hill

Telecommunications and privacy has been a recurring theme in these pages for several years. Again this year there are important developments to report—new legislative provisions to enhance the confidentiality of cellular communications and the Department of Communications' publication of a set of telecommunications privacy principles. Two other legislative initiatives get mixed reviews: the struggle for privacy regulations in the financial sector and amendments to the *Income Tax Act*.

Protecting cellular calls

In his 1990-91 annual report, the Commissioner alerted Canadians to the growing threat to privacy posed by interception of cellular telephone calls. Two highly publicized cases—one concerning a British Columbia cabinet minister who resigned after a newspaper printed extracts from calls he made on his car phone and suspicion that cellular communications were intercepted during the Meech Lake Conference—served to illustrate the point.

The Commissioner urged Parliament to act quickly to protect the privacy of cellular phone users.

There is good news to report. Last December the government introduced Bill C-109, amending the *Criminal Code* and the *Radiocommunications Act* to make it illegal to intercept private cellular phone conversations maliciously or for gain, and to provide for both civil damages and criminal penalties. The *Criminal Code* amendments also expand the definition of a private communication to include encrypted radio based communications.

Although the amendments do not ban cellular scanners, nor do they make it illegal to eavesdrop on cellular calls, they do give cellular telephones some of the protection of conventional "line-based" telephones.

Much as the Privacy Commissioner would like to take some credit for catalysing the legislative process, he suspects the intercepted

Wilhelmy-Tremblay call during the constitutional negotiations (and the ensuing media attention) did more to concentrate legislators' minds.

Some will argue that these measures do not go far enough because they do not ban scanning devices, an approach taken in the United States. While the Privacy Commissioner might prefer the American approach—and its clear statement that the interception itself is wrong—he is nonetheless gratified with any legislative measures to enhance the privacy of Canadians.

Telecom Privacy Principles

The second significant development in telecommunications this year results, in part, from an item in last year's report which discussed the privacy impact of new technological advances and the seeming futility of trying to devise technical solutions for each new technical marvel. The Office had begun work on broad privacy principles and commended this approach—borrowed from New York state—to the Department of Communications in December 1991, and to the Senate Transportation and Communications Committee in June 1992.

The combination of the Communications minister's commitment and his department's resources and expertise have produced a framework of privacy principles to guide the telecommunications industry. These principles emerged for the most part out of two significant events.

First, Bill C-62, the proposed new *Telecommunications Act* was introduced in February 1992. It sets out as one of eight policy objectives for the government:

“... to respond to the economic and social requirements of users of telecommunication services, including the protection of the privacy of individuals.”

Second was the caller I.D. decision by the CRTC. This decision, a reversal of an earlier verdict, put to rest perhaps the most controversial issue arising from the introduction of Call Management Services by the telephone companies. In the end, the CRTC required all companies in its jurisdiction to provide free per-call blocking for callers who did not want their numbers displayed.

Caller ID and cellular telephones are two good examples of the double-edged nature of technological advancement. In each case, important benefits and conveniences were made possible by new technology but, without some special arrangements, both carried with them significant potential loss of personal privacy. With privacy principles to guide it, the CRTC might have foreseen the problems with Call Management Services and dealt with them during the first review. This would have avoided the fuss and the need to review and overturn its earlier decision.

To implement the principles the minister has chosen a voluntary approach. There are obvious benefits. One; it allows industry to tailor a privacy protection framework that will suit its specific needs. Two; it provides a solution that transcends jurisdictional boundaries—all players whether private, public, provincially regulated, or federally regulated can participate. Three; it will be jointly funded by public and private concerns.

Key to the department's partnership approach is two bodies: a telecommunication privacy foundation and a telecommunications privacy council. The foundation will bring all the players together; the council (representing industry and consumers) will receive and adjudicate complaints.

However, this approach lacks specific statutory underpinnings and does not establish an independent dispute resolution mechanism—two elements necessary for an unconditional endorsement by the Privacy Commissioner.

Nevertheless, if industry commits to this approach, it may provide an adequate privacy protection framework. The Communications minister announced his willingness to consider a legislated solution if there is no support for this concept. With that added caveat, the Privacy Commissioner supports the initiative.

Amending the *Income Tax Act*

The Privacy Commissioner was also interested in amendments to the *Income Tax Act* and *Excise Tax Act* (bills C-92 and C-112). If enacted, these amendments would allow any Revenue Canada, Taxation official to use taxpayer information to supervise, evaluate or discipline a departmental employee.

The Commissioner raised two important concerns about these proposals. First; they designate Taxation employees as a new class of federal employee, subject to government monitoring and controls that differ from those of other employees. And second, they diminish existing confidentiality rights of all taxpayers because their files could be used in proceedings unrelated to the income tax process.

However, safeguards were included in the latter case to protect the confidentiality of taxpayer information in legal proceedings. The safeguards provide for in camera hearings, banning the publication of the information, concealing the identity of the taxpayer, and sealing the record of proceedings. Such a use of their files may, nonetheless, come as a surprise and source of concern among many taxpayers. The Commissioner recommended that prior to implementing such a system, Revenue Canada should consider acquainting taxpayers with the change.

Of greater concern was the first proposal designating Revenue Canada employees as a special class. Although the Commissioner recognizes the need to ensure the integrity of the tax system, he considered the proposals, as drafted, apply too broadly and open up the potential for abuse of employees' privacy. They could be

interpreted as allowing a supervisor the arbitrary power to retrieve and examine an employee's tax return at will. Thus, for example, should a Taxation employee be involved in a grievance proceeding against a supervisor (on matters unrelated to income tax collection), the supervisor could examine the employee's tax return and use it to threaten or intimidate.

Some occupations and professions often demand different or enhanced standards of behaviour of their members. However, the Commissioner thought that Taxation could achieve the desired level of integrity without resorting to such broad measures.

For example, the department could establish stringent criteria under which the management could examine employee tax files. It could define conditions of reasonable cause to avoid the potential for fishing expeditions in employees' personal and sensitive files.

As well, the department could devise a protocol allowing only senior program officials (not supervisors or personnel staff) to review employee files and determine whether to release information for the personnel uses envisaged. Revenue Canada should not contemplate such examination and disclosure for routine supervision and evaluation but only "for cause" to be defined in law.

At best, the present proposals represent a derogation from existing privacy rights without a corresponding protection of the employees' interests. Such measures should not be taken lightly and certainly not without a full and open public debate. They create the potential of a privacy underclass of citizens whose legitimate concerns are equally as important as the integrity of the taxation program. The privacy of their files is a priority consideration for Taxation employees. Any system that envisages diminishing that privacy demands stringent safeguards. A balance is necessary.

This apparent lack of balance between competing interests was not lost on members of the Commons Finance Committee. The amendments were initially voted down by the committee, but reinstated at the report stage by the government.

In letters to the Privacy Commissioner and the Committee, the department acknowledged that the proposals fundamentally alter existing confidentiality provisions, but insisted that

It is our duty to ensure that Revenue employees conduct themselves in a manner appropriate for persons who have privileged access to the tax system. While the vast majority do, it would be unfair to other taxpayers if a Revenue employee who had abused the system or who was demonstrably incompetent was shielded from normal disciplinary action simply because the relevant tax-related evidence could not be used or provided.

The department argued that the amendments provide additional privacy protection since taxpayer information could only be used if it is **relevant to**, and **solely for** a purpose related to supervision, evaluation and discipline. As well, the department proposed to issue guidelines to deal with the Privacy Commissioner's objections. Officials assured the Commissioner that both he and union officials would be consulted on the guidelines before they are finalized and implemented.

The Commissioner accepted the department's offer to work on a set of mutually-agreed safeguards, in cooperation with the public service unions concerned. This will mark the first time this Office has worked directly with a department to improve the privacy aspects of its employee administration process. The results seem certain to be of interest both to the bureaucracy and to Parliament. Pending the outcome, the Commissioner acknowledges Revenue Canada's ready response to his concerns.

Two further amendments also caused the Commissioner some concern; those to section 241 of the *Income Tax Act* proposing that an official “may” provide access to taxpayer information for the purposes of section 45 of the *Privacy Act* (and similar wording for section 295 of the *Excise Tax Act*). These provisions could have been interpreted to mean departmental officials had the discretion to refuse to disclose taxpayers’ information to the Commissioner’s staff during a complaint investigation.

Revenue Canada agreed that these sections should be interpreted simply as enabling department officials to allow the Privacy Commissioner to carry out his duties without Revenue Canada being in breach of those sections of the *Income Tax Act* or the *Excise Tax Act*.

Privacy in Banking

The Commissioner reported last year that a great divide may have been traversed with the introduction of two pieces of legislations—a bill dealing with banks and financial institutions, and a new Telecommunications law. As reported earlier, recent initiatives now offer more than a mere glimmer of hope that privacy will be adequately protected in telecommunications. The news is not as encouraging for the banking provisions. They seem to be snagged somewhere along the divide.

In April 1992, the Commissioner appeared before the Senate Banking Committee to urge Parliament to seize the opportunity to draft regulations that would protect privacy in the banking world. The Committee was quick to pursue this suggestion and with the help of Professor David Flaherty of the University of Western Ontario drafted a set of regulations. These regulations are based on existing *Privacy Act* provisions but adapted for the banking industry.

As promised, the Commissioner was invited to reappear before the Committee last December. He reiterated his strong support for

embodying basic privacy protection standards in the legislation. As well, he contended that no privacy protection scheme could command public confidence without an independent dispute resolution mechanism—one with the power to investigate complaints and to review both the information holdings and information management practices of the financial institutions. As of this date, the Senate Committee has not issued its final report.

A strong private sector lobby led by the Canadian Bankers' Association advocates a completely self-regulatory approach. The Commissioner while no great fan of government intervention for its own sake, continues to believe that basic common standards and independent oversight are necessary to guarantee fairness and transparency in this field.

...On the Streets

Privacy revealed: the Canadian privacy survey

For the first time in its ten-year history, the Commissioner's office has reliable analysis of Canadians' expectations, knowledge and fears about their privacy—and they feel “under siege.”

The results of the first broad spectrum study of Canadians' views about privacy are long overdue. They are dramatic confirmation of people's awareness and concern about the threats from technological, commercial and social changes.

Ninety-two per cent of Canadians expressed some concern about their privacy—52 per cent were “extremely concerned”—comparable to extreme concern about the environment (52 per cent) and unemployment (56 per cent) and well ahead of worries about national unity (31 per cent).

The majority of Canadians (60 per cent) feel they have less privacy than they did a decade ago—40 per cent feel “strongly” that their privacy has eroded. Four out of five respondents said that computers are reducing our privacy and 54 per cent are extremely concerned about the linking of personal information from one electronic data base to another.

Perhaps the most startling finding for the Commissioner's Office is that, whether or not they have ever read a privacy act or heard of a privacy commissioner (and as the survey says, few have) Canadians have put their fingers on the fundamentals of privacy protection. And the watchwords are knowledge, control and consent.

One of the key patterns evident in the findings is the greater the respondents' sense of control and knowledge of the process, the greater their level of comfort. This need to participate and control is evident in the following findings:

- 81 per cent feel strongly that they should be notified in advance when information about them is being collected;

-
- 83 per cent strongly believe that they should be asked for permission before information about them is passed from one organization to another;
 - 87 per cent strongly agree that when information about them is collected they should be told what it will be used for;
 - 72 per cent said that being in control of who can get information about them is extremely important, and
 - 67 per cent feel controlling what information is collected about them is extremely important.

The survey (entitled *Privacy Revealed*) also revealed a very strong desire for action. Although respondents were prepared to consider some creative approaches such as partnerships between government and business—and also to take responsibility themselves—it was clear that pure self-regulation by business (the status quo) was the least acceptable at 26 per cent. The strongest support was for the active involvement of government.

The survey was conducted by Ekos Research Associates Inc. of Ottawa on behalf of the Privacy Commissioner, AMEX Bank of Canada, Canadian Bankers' Association, Consumer and Corporate Affairs Canada, Communications Canada, Equifax Canada, Statistics Canada and Stentor Telecom Policy Inc.. Ekos surveyed 3000 Canadian households;—the results are valid within a range of +/- 1.8 points, 19 times out of 20. The study will establish a base line against which future studies can be measured.

A survey of this size and rigour would have been impossible for the Commissioner's Office alone and likely for the other federal partners. The Commissioner is grateful to Ekos Research for the quality of its analysis and the many extra hours spent; to Stentor Telecom Policy for the initiative, financial commitment and staff work, and to Communications Canada for the contributions of its policy staff. It would not have been possible without them.

...In the Courts

Privacy Commissioner v. Canada Post Corporation

For the first time in the *Act*'s ten-year history, the Privacy Commissioner has asked the federal court to review an institution's denial of access to personal information.

The Commissioner asked the court to determine whether the complainant has the right to know the identity of a witness who provided testimony against him during a grievance hearing, and on the basis of which the grievance was denied.

Canada Post initially denied the man both the name and the substance of the witness's testimony because it had been "prepared or compiled in the course of an investigation" and its release would injure the conduct of a lawful investigation (paragraph 22(1)(b)). He complained to the Commissioner. During investigation, Canada Post relented and provided the testimony but removed any identifying details and refused to name the witness.

The corporation argued that revealing the name would be "injurious to enforcement of any law" since the information was prepared during an investigation and it would identify a confidential source of information. It also maintained that revealing the witness's identity would offend the *Act*'s provision against disclosing personal information about someone other than the complainant (section 26).

The *Privacy Act* defines personal information as including "the views or opinions of another individual about the individual." In other words, if Mary makes a comment about John, that is John's personal information. The Commissioner has asked the court to consider the distinction between a confidential source who provides information during law enforcement and a witness whose testimony is heard as part of an administrative process. The court will also be asked to assess what harm disclosure could cause once this type of administrative investigation is completed.

No date has been set for the hearing.

During the year courts issued decisions in two cases dealing with privacy matters.

SINs for birth registration

The first concerned Prince Edward Island's requirement that newborn babies be issued a Social Insurance Number, reported in the Commissioner's 1991-92 annual report.

Briefly, a couple refused to apply for a SIN for their newborn baby and were subsequently denied all claims for the baby's medical care because she did not have a SIN (the province's health care number). The parents argued that requiring someone to have a SIN to be eligible for medical benefits violated the *Charter*, denied equal treatment under the law and breached a person's reasonable expectation of privacy.

The court ruled against the parents on each ground. However, of particular interest to this Office was the court's comment on the *Privacy Act* and its application to a 1970 federal-provincial agreement under which Employment and Immigration Canada issues SINs for births registered in PEI.

In the court's words, "...the province does not have the right to receive information on individuals' Social Insurance Numbers from the Government of Canada without the consent of the individual, as it has not met the provisions of subsection 8(2) of the *Privacy Act*."

The Commissioner reviewed the decision which buttressed his own suspicion about the validity of the 1970 agreement (made well before the *Privacy Act* came into force). He wrote again to EIC, this time asking it to stop issuing SINs on the basis of the old agreement. EIC and Health and Welfare Canada have both committed to recommending PEI stop using SINs as health numbers and have undertaken to help the province adopt its own

personal identifier for health care. However, EIC will await the outcome of the parent's appeal of the decision.

Patient access to medical records

In another case, the Supreme Court of Canada ruled that a New Brunswick patient had the right to see all the documents in her medical file, not just those created by her current doctor.

The doctor had provided copies of all the documents she had prepared, but refused to allow the patient to examine any created by other medical practitioners. The doctor considered that would have been unethical since the records were someone else's property.

The court concluded that the physical records were indeed owned by the doctor. It also affirmed the physician's duty to protect the confidentiality of a patient's medical file unless the patient or the law authorized otherwise. But the court made it clear that the doctor-patient relationship "is fiduciary in nature" and information a patient reveals to a doctor "remains, in a fundamental sense, one's own."

The court observed that this "trust-like beneficial interest of the patient in the information indicates that, as a general rule, she should have a right of access to the information and the physician should have a corresponding obligation to provide it."

The right is not absolute. The court acknowledged that a doctor might have reason to believe it would not be in the patient's best interest to see some material. However, the decision puts the onus on the physician to justify denying a patient access.

While the case has limited immediate impact—applying only to those jurisdictions without specific legislation on patient access—it is important re-enforcement by the nation's highest court of individuals' proprietary interest in their personal information.

...In the Labs

Biotechnology update

Two major developments occurred in drug testing at the federal level this year. In May 1992, regulations authorizing a wide range of drug testing programs in the Canadian Forces came into effect. In November, the *Corrections and Conditional Release Act* came into force, also authorizing a wide range of testing programs for inmates and offenders released into the community.

Drug testing remains a concern of this Office. Alcohol, not drugs, poses the greatest threat to workplace and public safety. Yet, the government continues its march towards drug testing.

Unlike alcohol testing, drug testing (urinalysis) cannot measure impairment. Even alcohol testing is an imprecise measure and the legal limit is arbitrarily set. Drug testing can measure only past drug use. It cannot tell how much was used, exactly when (only within days at best, and weeks at worst), or whether the drug impaired the user at the time. Most important, it cannot tell whether the user is **now** impaired. Thus, drug testing cannot reveal the only information that has any relevance—present impairment.

Simply put, drug testing will not tell air travellers whether their pilot is impaired. It will tell them only that the pilot has used a drug sometime in the past—information no more useful than knowing that their pilot may have had something to drink or been impaired by the flu or jet lag within the last month or week. Drug tests give no indication of the pilot's present ability to fly safely.

This Office is not insensitive to concerns for public safety. It accepts that some circumstances justify privacy intrusions. The legislation allowing the taking of breathalyser tests for alcohol impairment is a good example. But drug testing has no such justification. Instead, it represents a major new type of state-sponsored intrusion into the human body. Even persons charged with murder cannot be forced to surrender bodily

substances for forensic purposes, so great has been the law's protection of the integrity of the human body.

In short, drug testing is a major intrusion that is not offset by any significant benefits.

Canadian Forces' testing programs

Of particular concern is the drug testing program now underway in the Canadian Forces. This Office's 1991 report, *Drug Testing and Privacy*, questioned the need for testing within the Canadian Forces. If anything, our conviction that testing is not justified has strengthened. The results of a 1989 survey of Forces' members demonstrated clearly that use of alcohol, not illegal drugs, poses the greatest potential drug-related safety problem in the CF. The simplest way to explain the 1989 survey results is as follows: for every 1000 members of the Canadian Forces asked which drugs they had used in the past month

- three would say they had used LSD;
- five would say they had used cocaine;
- 25 would say they had used marijuana, and
- 780 would say they had used alcohol.

If there are drug-related safety problems in the CF, they stem to a far greater extent from alcohol, not illegal drugs. Yet the drug testing program almost exclusively targets the illegal drugs. The 1989 survey showed clearly that illegal drug use in the Canadian Forces is not of such magnitude that it justifies a massive intrusion into the bodies of its members through drug testing. The Commissioner has expressed his reservations to National Defence officials and written to the Chief of Defence Staff, all to no apparent avail. The Commissioner does not intend letting this issue drop.

A subsequent "blind" test (on December 8, 1992) collected more than 5,500 urine specimens at 15 locations in Canada and in

Germany. These samples were then analyzed for cannabinoids (e.g., marijuana), cocaine, opiates, amphetamines and phencyclidine (PCP).

The results of the blind testing (although not strictly comparable with the results of the earlier survey), support the Office's position that members' rates of drug use are very low, and that the massive testing program introduced to detect those drugs is an unwarranted intrusion.

Testing inmates and parolees

The *Corrections and Conditional Release Act*, which came into force in November 1992, introduces a broad range of drug testing programs for inmates and those who have been released into the community. The justifications advanced for testing inmates and parolees differ from those for testing others. The drug trade in prisons is said to lead to increased violence and coercion within prisons. Reducing the demand for drugs through drug testing, it is argued, may help reduce these problems.

This Office certainly does not oppose reasonable measures to reduce violence within prisons. However, it remains to be demonstrated that drug testing will accomplish this. If it does, the violation of privacy may be warranted. If it does not, we hope that the Solicitor General of Canada will be sufficiently open-minded to reconsider the program.

Drug testing in prisons could pose one particularly grave danger. Drug users worried about being caught may switch from drugs that can be detected long after use (like marijuana) to those detectable for only a short period (like heroin and cocaine). This means switching from a smokable drug to one usually administered by injection. Given the scarcity of syringes (and syringe cleaning materials) in prisons, this could greatly increase the risk of HIV infection. While not strictly a privacy matter,

anything that increases the risk of HIV infection is yet one more argument against violating individual privacy through drug testing.

Transportation industry employees

A third major testing issue concerns the transportation industry. As this report goes to press, drug testing legislation aimed at safety-sensitive transportation positions appears unlikely to even be introduced before Parliament's summer recess.

Nevertheless, the Commissioner's concern bears repeating—the proposed transportation testing program constitutes overkill. It also unnecessarily sacrifices hard-won privacy rights. There is good news: the minister of transport has decided not to proceed with the department's planned random testing. Still, several other aspects of the testing program remain objectionable.

Testing athletes

The Office continues watching developments in drug testing in sport. Athletes too have basic human rights, including the right to privacy. Drug testing programs may help to make sport somewhat more fair, but at what cost? Particularly worrying is the response of a few to a recent Canadian Centre for Drug-free Sport questionnaire—they identified blood testing for drugs as an appropriate activity for the Centre. Urinalysis is intrusive, but at least it does not involve entering a person's body to remove body fluids, as blood testing would. It is frightening to think that some people will contemplate violating the very physical integrity of human beings, an integrity protected for centuries by law, in the name of men and women playing games.

Genetic Testing

The Office continues to follow rapidly occurring developments in genetic testing and their impact on privacy. Although our 1992 report, *Genetic Testing and Privacy*, has received national and

international praise, genetic privacy concerns have fallen behind other public issues. The immediacy of the dangers of unregulated genetic testing risks being overlooked.

Genetic technology will not wait for us to catch our breath. Genetic discoveries are breaking at an ever-increasing rate. Scientists and biotechnologists will continue to develop new, cheaper and more accurate genetic tests to identify physical and behavioral traits. Some traits, if revealed to employers, insurers and governments, will almost certainly stigmatize individuals or precipitate discrimination against them simply on the basis of their genes.

By waiting, we come ever closer to losing control over our own genetic information—information about the very essence of our beings. The Commissioner urges Parliament to take up this issue before a post-Orwellian genetics free-for-all engulfs us.

...Here and There

Regular readers of these reports will know that the Office monitors privacy protection elsewhere in this increasingly interconnected world. The past year has seen progress both at home and abroad.

In the provinces: Quebec

In December 1992, the Quebec government introduced Bill 68, an act to extend privacy protection to the private sector.

If passed, this will be the first legislation in North America to regulate private sector collection, use and disclosure of client and employee personal data.

The legislation would require businesses to limit collection of personal information to specific stated purposes. Clients could not be denied goods or services for refusing to provide personal information unless the details were required by law or to fulfil contractual obligations.

The bill would also require businesses to tell clients what information is held about them, to keep the data accurate, up-to-date and complete, and to obtain the subject's consent for any disclosures to third parties that are inconsistent with the stated purpose (unless specifically allowed by the legislation).

Consumers will be able to opt out of telemarketing or mail solicitation and to find out where the business got their personal information. And companies must have appropriate security measures in place to protect the confidentiality of personal information.

Specific provisions deal with credit reporting companies which must register with the provincial access and privacy commission and publish their activities in the newspapers. The bill sets out fines for non-compliance ranging from \$1,000 to \$10,000, depending on the offence.

The Quebec privacy commission will play a lead role in overseeing administration of the act. It will investigate complaints and issue binding decisions (although questions of law and jurisdiction may be appealed to the courts). The Commission will also have an education mandate and can encourage and help business develop internal privacy codes.

A legislative commission held public hearings and is now reviewing the bill and considering specific amendments.

At least one question remains to be answered: will the legislation apply to federally regulated businesses such as banking, transportation and communications? If so, will these sectors provide the same level of privacy protection to other Canadians?

British Columbia

In June 1993, British Columbia's legislature passed the province's first *Freedom of Information and Protection of Privacy Act*.

The act (which takes effect in October 1993) is broadly similar to other provincial legislation and will apply to BC government bodies. However, before even taking effect, the act is being amended to extend its provisions in October 1994 to local government bodies such as school boards, hospitals and municipalities. Other amendments would see self-governing professional bodies covered by Spring 1995.

Complaints will be handled by a commissioner—part ombudsman, part tribunal—allowing for both mediation and (if it fails) enforceable orders. Unlike the federal ombudsman, the commissioner will have access to Cabinet confidences to assess the validity of exemption claims. He or she has a specific mandate to carry on education and research. However, the commissioner too must live with time limits; reviews must be completed in 90 days. There are some undeniable benefits to having order

powers—they will allow the commissioner to impose deadlines on reluctant government agencies.

Overseas: the European Community Draft Directive

Of course, privacy developments can have implications well beyond national or regional boundaries.

The most obvious illustration is the European Community's (EC) draft directive on protecting personal data. Earlier reports have cautioned Canadian governments and business about the potential implications of strict European privacy rules on transfer of personal data in and out of the community—particularly to North America.

During the past year, the EC directive came under intense pressure from business, particularly the direct marketing and financial sectors. Business identified several problems: the directive's restriction on transfer of personal data to non-EC countries without "adequate" protection; the need for the subjects' express consent before their data is processed or transferred; "unnecessarily burdensome" obligations to notify the data protection authorities; and lack of flexibility for member states to use various kinds of regulation or codes to implement the data protection principles.

The lobbying had some effect and, in October 1992, the EC issued an amended directive. The revised version continues to require "adequate" protection in non-EC countries receiving EC residents' data. And it has dropped any formal distinction between the public and private sectors—the rules are the same. However, there is added flexibility. The directive now allows transfers if the subjects consent, if the data is needed to satisfy a contract between subject and controller (notice must be given to the subject), and if an important public interest or the vital interests of the subject are at stake.

The amended directive will also allow EC countries to consider the type of data, the reason for processing, any sectoral codes, as well as legislative provisions, and even “professional rules” when assessing the “adequacy” of non-EC countries privacy protection.

It is not clear how Canada’s patchwork of public sector legislation and private sector codes (or statements of good intent) will measure up.

OECD Experts Privacy Briefing

Technology is usually blamed for eroding rather than enhancing privacy. But a November 1992 meeting of the OECD (Organization for Economic Cooperation and Development) turned the problem on its head and looked at the potential of technology to protect personal data. The OECD invited several experts to brief government participants on using new technologies and processes to protect personal data in electronic systems.

Some of the technical possibilities include encryption (coding), trusted systems (specially designed to meet specific security objectives), blind signatures and electronic cash (verifying financial transactions without tracing the individual) and networks which allow transmissions between parties without their being “observed.” It is unlikely that any system will be foolproof but these meetings are an important step in building controls into the systems themselves. The group expects to meet again.

As well, the OECD passed its new Guidelines on Information Security Systems which will soon be released.

Privacy in Hong Kong...

The Hong Kong government recently issued a discussion document examining the Crown Colony’s current privacy protections and outlining a framework for a privacy protection bill. The draft was produced by a Law Reform Commission

sub-committee, representing academia, law, telecommunications, banking, trade, police and the media.

The draft contains the eight OECD principles and much of the spirit of the latest EC draft directive. There is a comprehensive description of what constitutes personal information and its jurisdiction will include both the public and private sectors. The draft also deals with sectoral codes, data matching, direct marketing, personal identifiers, and transborder data flow. Two of its strengths appear to be provisions for ensuring that data subjects consent to uses and disclosures, and allowing individuals to opt out of direct marketing activities.

With Hong Kong's reversion to mainland Chinese control in 1997, the future of the proposed bill is uncertain.

...and New Zealand

New Zealand is in the midst of considering a comprehensive privacy act to replace a number of statutes, each with limited jurisdiction. The bill contains 12 privacy principles, expanding on those contained in the OECD principles and the EC directive. It will cover both the public and private sectors and it tackles such subjects as private sector codes of practice, public registers (for example, electoral lists) and data matching.

The bill would allow the privacy commissioner to issue emergency codes of practice. It also sets out comprehensive data matching requirements for the public sector, requires users to verify the accuracy of personal data before processing, and establishes a broad scheme of damages to compensate those whose privacy is breached.

There are, however, some notable omissions: organizations have substantial discretion to determine what are "trivial" demands and they may charge fees to process access, correction and notation

requests. And it appears that criminal offenders will have no access and correction rights.

The bill is awaiting second reading and is expected to take effect on July 1, 1993.

...In the Private Sector

The CSA model code

Last year we reported the Canadian Standards Association's initiative in developing a model privacy code to serve as a minimum standard for private sector handling of personal information. The model code holds promise for some meaningful privacy protection without resort to legislation.

CSA formed a committee whose goal is to develop and then promote a model code based on the OECD guidelines. The members (including this Office) represent finance, insurance, direct marketing, telecommunications, information technology, utilities, credit reporting, consumers and federal and provincial governments.

Work continues apace. Committee working groups have prepared documents explaining each of the OECD principles in everyday language and identifying the issues that must be dealt with to implement each principle. A drafting committee will now amalgamate and edit all the material into a single draft model code which is expected to be ready for committee review later this year.

One important aspect of any code is the oversight mechanism. The committee expects to make specific recommendations on several possible options for registering or certifying industry specific codes.

Privacy staff were also resources for CSA's consumer advisory panels which provide input and public review of the standards. Recommendations from these panels will help the committee reflect the privacy concerns of the wide range of interests and occupations beyond its immediate membership.

Canadian Direct Marketing Association

Also reported last year was the CDMA's decision to develop its own specific privacy code (CDMA is also a member of the CSA group).

The CDMA has done it. The code, released in January 93, was developed following two years of research and consultation with consumers, industry and privacy experts. Prior to the code, CDMA had offered consumers the option of removing their names from all CDMA members' lists. But the new code goes further. It gives consumers a means of controlling the transfer of marketing information about them by allowing them

- to decline to have their names used;
- to know the source of their information, what information it holds and to request correction of errors;
- to control the subsequent use of their information by third parties;
- to be reassured about the security of their information;
- to benefit from more stringent protection for sensitive information, and
- to complain to the CDMA if a member breaches the code.

The code demonstrates what commitment to an idea can produce. CDMA members understand the importance of consumer confidence, control and consent for the health of their industry. The code is not perfect; there are no limits on collection (as envisaged by the OECD guidelines) and the oversight mechanism is not independent. Nevertheless, the effort deserves a round of applause from consumers and privacy commissioners alike.

...In the Office

Investigating Complaints

There were no surprises this year. The number of new complaints climbed to yet another record total of 1,579—a 13 per cent increase. However, investigators closed 1,440 cases during the year, almost double last year's productivity. Of the closed cases, 590 were well-founded, 757 not well-founded and 104 discontinued.

Complaints about time limits and denial of access made up 86 per cent of all complaints received. Many institutions have blamed their poor track record on staff cutbacks caused by the government's drive to reduce expenditures. The result is slower service to applicants.

How Institutions Measured Up

Here too there are few surprises. Over 85 per cent of the new complaints were against virtually the same departments as in previous years: Correctional Services (CSC), Revenue Canada, Taxation, Employment and Immigration Canada, Canada Post Corporation (CPC), Canadian Security Intelligence Service (CSIS), Royal Canadian Mounted Police (RCMP), Revenue Canada, Customs and Excise, and National Defence. New to this year's top ten are Transport and Health and Welfare Canada.

Health and Welfare Canada

New complaints against Health and Welfare climbed to 132 this year (90 access, 28 time limits and 14 others) from 40 in 1991-92. The vast majority concerned information held by Income Security Programs—Canada Pension Plan, Family Allowances and Old Age Security—programs that maintain files on virtually every Canadian. The department was also the subject of many complaints about tardy responses to requests—18 of 37 completed complaints concerned time limits, all but two of which were well-founded.

Canada Post Corporation

The number of new access and time limits complaints against Canada Post were similar to last year's—54 and 22 respectively. However, the corporation continues to be the target of many complaints about its collection, use, disclosure and retention of employee records. These 43 privacy rights complaints make up 36 per cent of Canada Post's total case load of 119—the highest number of any government agency.

Two years ago there was praise for Canada Post, despite having the questionable honour of the office's most important client. Almost 80 per cent of its complaints were not well-founded, many related to its administration of the employee attendance and leave policy and its modified duties program for employees unable to carry out their normal functions due to injury or illness.

This year more than half of the complaints against CPC focused on its inappropriate use of exemptions (half were well-founded), and delays in processing (22 of 24 well-founded).

All but a handful of complaints originated from CPC employees in Ontario (particularly in Metro Toronto and southern Ontario) who are involved in labour relations disputes. Some CPC labour relations officials see an inherent unfairness in allowing employees in labour disputes to use the *Privacy Act* to obtain documents germane to their grievance, while there is no parallel right for CPC management to obtain access to the unions' files.

This view that the *Act* is a pawn in labour relations disputes has made it very difficult to resolve some complaints. An illustration is the office's first case which asks the court to review Canada Post's refusal to disclose the identity of a witness who provided information in a grievance matter (see *In the Courts*).

Other departments

More than 100 of the 172 complaints investigated against Revenue Canada, Taxation were filed by one individual, all related

to time limits. Customs too had problems meeting the 30-day deadline: 36 of the 44 against that department were well-founded.

The RCMP is to be commended for its efforts to follow the letter and spirit of the access provisions of the *Act*. Of the 47 time limits, denial of access and corrections complaints investigated this year, none were well-founded. CSIS, too, responds promptly and properly. Only two of 89 complaints were well-founded, but both were resolved.

Still, it is discouraging to have to report that after ten years administering the act, many departments still have difficulty responding to requests properly and in a timely fashion.

Origin of Completed Complaints

Newfoundland	8
Prince Edward Island	3
Nova Scotia	27
New Brunswick	30
Quebec	153
National Capital Region Quebec	13
National Capital Region Ontario	156
Ontario	588
Manitoba	63
Saskatchewan	55
Alberta	101
British Columbia	216
Northwest Territories	2
Yukon	19
Outside Canada	6
TOTAL	1,440

Notifying the Commissioner

Although the *Privacy Act* generally prevents federal organizations from disclosing personal information without the person's consent, there are exceptions. Two of these oblige the organization to notify the Privacy Commissioner: a release in the "public interest" or one which would clearly benefit the person concerned. There were 48 notifications this year.

The *Act* requires the head of the organization to determine what is in the "public interest", not the Commissioner. The Commissioner's role is to review the proposal and to notify the individual concerned if that seems appropriate. The Commissioner has no power to prevent a release; however, if he strongly disagrees he may initiate his own complaint. The individual also has no avenue to block release but does have a right to complain to the Commissioner, albeit after the fact.

Staff examines these notifications, leaving the Commissioner free to consider any ensuing complaints.

Assessing the public interest can be a tough call for department heads, as some of this year's notifications illustrate.

HIV status disclosed

Correctional Service Canada (CSC) advised the Commissioner that it would disclose the HIV status of a man alleged to have sexually assaulted two young girls. The man, on parole at the time, had refused the fathers' request for the results of blood tests he took voluntarily when he was arrested.

Since the test results were negative, CSC wanted to assure the families that their children had not been exposed to the HIV virus. However, the Commissioner cautioned CSC that the negative test did not necessarily mean the children's health was no longer at risk. The HIV virus can remain undetected for years after the person is exposed. The Commissioner urged CSC to point this out

to the parents. CSC agreed and the Commissioner advised the man of the disclosure.

Nurse's name to professional association

In another HIV-related case, CSC advised it would give the Registered Nurses Association of British Columbia the name of a nurse who had left an HIV-contaminated syringe on the counter in a federal penitentiary. Another nurse then used the syringe to draw blood from a second inmate.

CSC's board of investigation recommended reporting the incident to the association. Nurses are obliged to report any breaches of their code of conduct to their association but the nurse's union had advised her to refuse. CSC considered it in the public interest to ensure professionals comply with their code of conduct and advised the association. The Commissioner wrote to the woman to ensure that she understood the government's obligations and her rights under the *Privacy Act*.

Team member's passport details to Olympic organizers

A last minute opportunity for the Canadian women's fencing team to compete in the Barcelona Olympics prompted an urgent call to External Affairs Canada for passport information on a team member.

The team had not qualified in the top 12 during preliminary competitions and members had dispersed. But when two qualifying countries failed to field complete teams, the Canadian women were invited. Organizers scrambled to re-assemble the team and to provide passport information immediately to Olympic officials for security and identification. When organizers could not reach one of the members, they asked External to provide the woman's passport number and expiry date.

External concluded that there was a public interest in having the team compete and a personal benefit to the team member. The department advised the Commissioner it would release the information. She was reached 12 hours later.

Electoral lists to political parties

A 1992 privacy compliance review of Elections Canada revealed that electoral lists were routinely being disclosed to political parties and candidates in the “public interest” without notifying the Commissioner. As a result of the review, the Commissioner received his first formal disclosure notice in January 1993.

The lists are assembled from door-to-door enumeration conducted during an election campaign. They contain the last and first names, sex and address of each eligible voter in the riding and are available in paper or electronic form. Political parties and candidates use them for promotional mailings, door-to-door canvassing and to solicit contributions. The current lists are particularly valuable since voters were enumerated recently for the Constitutional referendum.

Elections Canada receives many requests for the lists but provides them only to political requesters in the interest of candidates reaching constituents during an election campaign. The Commissioner is satisfied as long as the lists are used only for election purposes.

Nepotism allegations prompt release of personal details

A competition for customs inspectors in Winnipeg and Emerson, Manitoba led to allegations of favouritism in the *Winnipeg Free Press*. The Public Service Commission (PSC), which hires all federal public servants, advised the Commissioner that it had investigated the allegations and intended to release its report.

The PSC received more than 1,000 applications for the job openings at Revenue Canada, Customs and Excise. After an initial screening, customs officials interviewed 279 candidates who had passed the written test. The 20 qualified candidates were ranked in order of merit and 11 were offered positions.

Several unsuccessful candidates complained that at least three of those hired were relatives of Customs superintendents. Local media reported the allegations and other complaints surfaced—25 in all—including one from the Customs employees' union.

Given the seriousness of the allegations—and the PSC's mandate to uphold the merit principle in public service hiring—the PSC concluded that there was a clear public interest in a full accounting of the process. The report contained the names of all qualified candidates who were related to Customs employees, the position titles (but not the names) of the employees to whom they are related, and brief general summaries of the employment experience of a number of the applicants.

Unfortunately, the Privacy Commissioner was not notified until the day after the report was released to the newspaper, giving him no opportunity to alert the individuals to the probable publicity. PSC acknowledged the error but felt pressured to deal with the continuing media inquiries. The Commissioner decided to write to all those involved to explain the process and their rights under the *Privacy Act*.

Petro Can shareholders not disclosed

Supply and Services Canada (SSC) advised the Privacy Commissioner that the Information Commissioner had recommended it release the names and last known addresses of shareholders of Petro Canada Enterprises Inc. to an “investigative accountant.”

The department denied the accountant's Access to Information request because the information was personal and therefore exempt. The accountant complained to the Information Commissioner, arguing that it would benefit the shareholders if he could use the SSC lists to find them and—for a fee—obtain the moneys owing.

SSC holds the lists because the company was dissolved in 1983 and the value of the unredeemed shares (\$120.14 each) was paid into general government revenues. Registered owners may claim the money from SSC.

Apparently SSC had written to each shareholder at the wind-up of the company explaining the arrangement for cashing the shares. It also placed advertisements in major Canadian and foreign newspapers. Approximately 80 per cent of the shares have been redeemed and the department continues to receive claims from individuals on its lists. Following the complaint, the department mailed another reminder to shareholders. It argued that any shareholder who is unsure how to obtain the money need only contact Petro Canada or any stock broker.

There is a public interest in ensuring that the government makes reasonable efforts to locate those for whom it holds money. However, the Privacy Commissioner had reservations. He questioned whether that interest was best served by disclosing the information, without shareholders' consent, to a third party who intends charging a finder's fee of 15 to 40 per cent of the shares' face value. The disclosure seemed to served the accountant's interests more than the shareholders'.

Nor would the disclosure guarantee that all shareholders' interests would be served. The Commissioner doubted that it would make economic sense for the accountant to attempt to find at least half of the shareholders who hold three or fewer shares. As well, 60 per cent of all those on the list live outside Canada.

A second concern was how SSC would protect shareholders from subsequent use or sale of the lists. Once released, there is no legal means for the government to prevent third parties from duplicating, selling or otherwise using the information.

Finally, the Commissioner wondered how the accountant expected to find the shareholders using the same addresses as SSC. If there was a way, he encouraged SSC to use it and save the shareholders the third party's fees. Both Commissioners agreed that SSC needed to be more aggressive in communicating with shareholders—however the Privacy Commissioner was unconvinced that disclosure to a third party was the best remedy.

Although the accountant did not get the lists he wanted, his access complaint prompted the department to write again to all shareholders and to consider other ways of reaching those who do not respond.

Inquiries

Inquiries also increased again this year—by 10 per cent to 5,183. Of these, 4,865 were telephone calls, 274 letters and 44 personal visits.

Almost 55 per cent dealt with individuals' rights under the *Act* but about 20 per cent concerned privacy matters over which the Privacy Commissioner has no jurisdiction—other public sector organizations or private businesses. The remainder had been mis-directed or had nothing to do with privacy. Although many of the questions are outside the office's mandate, inquiries officers redirect callers to the appropriate organization or department.

Several callers were concerned about postal employees recording their identification card numbers when they received parcels and registered mail. The office reviewed Canada Post's procedure which requires anyone picking up parcels or registered mail to produce acceptable identification, and the postal employee to record the details in a ledger.

The Commissioner agreed that Canada Post must check identification to ensure that the person claiming the parcel is the intended recipient. The information is logged to provide a trail in case valuable goods or documents go astray. Privacy staff also confirmed that delivery registers are kept in an area not accessible to the public.

Inquiries officers continue dealing with many calls concerning the collection, use and disclosure of personal information by financial institutions. Since the banks are not subject to the *Privacy Act*, and the Office of the Superintendent of Financial Institutions does not deal with complaints about information practices, privacy staff must refer callers back to the financial institution—each of which has its own policy on management and use of personal information.

Inquiries officers often must explain that the *Act* deals with just one facet of privacy. For example, a man returning recently from

an overseas assignment, complained to the Commissioner about customs officials' rudeness and of their searching his personal files and belongings. He wanted to know his rights under the *Privacy Act*. Privacy staff explained that the *Customs Act* authorizes customs officers to examine goods and mail, and their rudeness is not covered by the *Privacy Act*.

Sometimes callers ask that their complaint be handled informally. An employee of a company participating in a work sharing program with Employment and Immigration Canada (EIC) was concerned that EIC sent documentation to the employees through the employer.

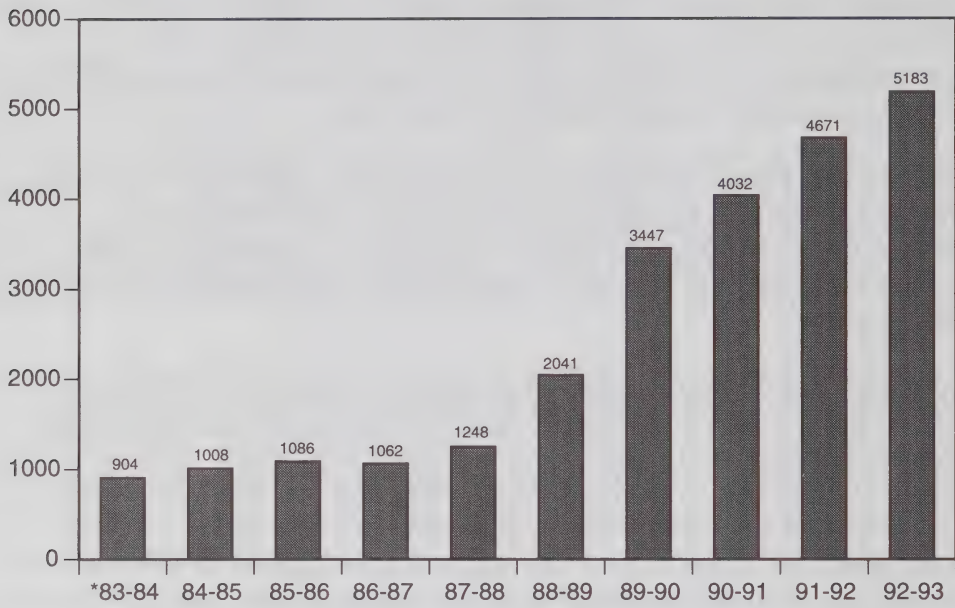
Although the company needed to examine employees' benefit statements to make the proper wage adjustments, the caller did not think it needed to see the employees' Telephone Access Code (TAC). This is a personal identification number which gives UI recipients access to information about their benefits over the telephone. EIC looked into the problem and agreed to remove the access code from the documents. It advised employees to change their TAC number.

Three callers asked whether a Moneymart, a video store and a large appliance store were allowed to take identification pictures of them. There is no legislation covering this situation. Is picture taking a new fad?

Inquiries about the SIN continue—549 this year. The Office's advice to anyone not wanting to provide their SIN to private businesses, landlords, or organizations not subject to any legislation covering the SIN, is to ask:

- Do you need my SIN to comply with a legal statute or regulation?
- Why do you need it and how will you use it?
- Will you keep it confidential?
- What are the consequences if I refuse?
- Would you accept another ID?

Inquiries 1983-93



* 9 Months

Some Cases

Job competition notes accessible

A complaint against the Department of Justice established an important precedent for access to handwritten notes taken by board members during job competitions.

A man asked the department for copies of all material gathered during his job interview. He complained to the Commissioner when Justice could not find the interviewers' notes.

The investigator found that all the selection board members took handwritten notes to help rate the candidates during the interviews. The notes taken by three board members were destroyed once the hiring process was completed. The fourth member (a staffing officer) recalls including her notes with the documents transferred to personnel when she left the department shortly after the interviews. However, a search of the department's staffing files found nothing. The department assumed the notes were inadvertently lost or destroyed.

While the Commissioner was prepared to concede that all employees occasionally make personal notes which cannot be considered "under the control" of their department, he was not persuaded that this was such a case. In his view, selection board members' notes are made to choose a candidate—an administrative purpose—and should become part of the staffing file. This means they are accessible under the *Privacy Act*.

After extensive consultations, Justice finally accepted the Commissioner's position. The department was unable to establish the exact content of the notes made about the complainant. However, it admitted that since the selection board considered the notes in reaching its decision, they had been used for an administrative purpose and should have been retained and made available to the complainant. Since they had not been kept, the Commissioner considered the complaint well-founded.

As a result of this investigation, Justice assured the Commissioner that it would require future selection boards to retain “notes made by members and used in the decision-making process.” The handwritten notes will be given to the personnel representative and become part of the final board report (unless they are incorporated verbatim). The Commissioner agreed with the department’s observations that the ramifications of the case were important enough to mitigate the delay.

Disciplinary notice not for union

An employee of Employment and Immigration Canada (EIC) complained to the Commissioner that his manager improperly disclosed disciplinary information about him to another employee during the October 1991 strike of the Public Service Alliance of Canada (PSAC).

The investigation revealed that the complainant was a “designated employee”, meaning he was required to work during the strike. However, one morning he failed to report for work and was seen later on the picket line. His manager wrote a letter reprimanding him for being absent without authorized leave, and attempted to give it to the complainant. He refused to accept it.

After advising him to report to work immediately (and the financial implications of refusing), the manager put the letter on the complainant’s desk. He also gave a copy to the PSAC union strike coordinator, who was the complainant’s local steward.

The Commissioner agreed that an employer has the right to tell the union official that a member is engaged in an unlawful strike but it did not have the right to give her a copy of the written reprimand, showing what disciplinary action would be taken. The Commissioner considered the complaint well-founded.

No medical details during reference checks

Another EIC employee complained to the Commissioner that the department improperly collected confidential and inaccurate medical information about her during a reference check with a supervisor, then used it to eliminate her from the list of qualified candidates.

The investigation confirmed that during a job competition in one of its employment centres, EIC staff conducted telephone reference checks with qualifying candidates' most recent supervisor. Asked if the complainant's attendance and punctuality were satisfactory during the past year, her supervisor provided specific medical details which were then recorded on the file.

Collecting information about illnesses or injuries during reference checks poses potentially serious privacy problems. It can harm the individuals by revealing gratuitous details about the person's health or life. The Commissioner was concerned about the accuracy of any medical information collected during the process, as well as the validity of any conclusions that staff might draw based on such medical data.

The *Privacy Act* prohibits collecting personal information unless it "relates directly to an operating program or activity" of the department. EIC conducts literally hundreds of staffing actions every year so it is inevitable that it will occasionally be offered unsolicited medical information during reference checks. Nevertheless, the Commissioner considers it the department's responsibility to ensure that it does not collect more personal details than it needs simply to assess a candidate's record for attendance and punctuality.

The Commissioner concluded that the medical information was not required for the staffing action and that the complaint was well-founded. However, he dismissed a second complaint that EIC had misused the information when it became apparent that it was

the complainant's attendance record (which was relevant) that made her unsuitable for the job.

EIC removed all the supervisor's references to her illness from the files. In addition, it agreed to publish guidelines to remind managers about the proper way to conduct reference checks in keeping with both the *Privacy Act* and the *Canadian Human Rights Act*. The Commissioner considered the matter resolved.

Need court order for disclosure

An employee of Correctional Service Canada (CSC) complained to the Commissioner that her director disclosed to a third party a copy of a security investigation report containing personal information about her.

The director confirmed that he had given a copy of the woman's report to the director of an after-care agency under contract to CSC. He had provided the report at the agency's request because the complainant had filed a lawsuit against the organization.

The Privacy Commissioner concluded that none of the disclosure provisions of the *Privacy Act* justified this release. The *Act* allows personal information to be released in response to a subpoena or court order but the outside agency had obtained neither. The Commissioner concluded that the disclosure was unwarranted and considered the complaint well-founded.

Legal guardian must consent for minor

A man complained to the Commissioner that External Affairs denied him access to his son's passport records. The father felt that since his son was a minor, he was entitled to see the records.

The Commissioner was satisfied that the passport information was personal information about the son. The *Act* allows personal information to be disclosed only to the subject of the information

unless he or she consents to release to a third party (there are some specific exceptions). Since the son is a minor, the *Privacy Regulations* require the consent of the individual's legal guardian—in this case, the complainant's former wife.

The Commissioner believed that External Affairs had acted properly in refusing the complainant's request and considered the complaint not well-founded.

SIN optional for job-seekers

A man's complaint that Employment and Immigration Canada (EIC) misused his social insurance number (SIN) has led to a change in the way EIC registers clients seeking employment.

The complainant refused to provide his SIN when registering for summer employment and wanted to know why it was necessary. He alleged that his question was referred to a manager who then retrieved the man's SIN from departmental files before talking to him.

EIC claimed that it is reasonable for a CEC manager, before returning a client's phone call, to use the client's SIN to retrieve the file and thus be better prepared to respond to the client. The Commissioner was satisfied with the explanation and found the complaint to be without merit.

However, EIC officials were asked why clients must provide the SIN when simply registering for employment. They assured the Commissioner that the intent is simply to provide the broadest range of services EIC has to offer its clients. The SIN is the only practical means for identifying and referring clients with particular skills to suitable job openings.

Nevertheless, EIC did agree to dispense with collecting the SIN when the client objects. However, staff will caution those clients that not having their SIN will limit the services EIC can provide

and could mean lost job referrals. The choice of providing the SIN will rest with the client.

HIV poster display “careless”

The Privacy Commissioner received a complaint from the B.C. AIDS Network that the RCMP had posted photographs and descriptive details about five HIV-positive individuals on a bulletin board in the local detachment. Someone had seen the information and told one of the individuals who complained to a local AIDS support group.

The Commissioner investigated to determine whether the RCMP should have collected the information that the individuals were HIV-positive, and to assess how the Force was using it and whether the disclosure was proper.

The investigation established that the photographs and details were collected from the detachment’s own operational files. Police files identified all five individuals as known repeat offenders with a propensity to violence. They were considered to pose a threat to police and guards and all had volunteered that they were carriers of the HIV virus.

Although the individuals were well known to the detachment’s full-time guards, staff suggested posting the information in the guards’ office where 10 casual guards (who replace full-time staff who are on leave or sick) would see it.

The investigator found that prisoners and the public do not enter the guards’ office. In fact, even police officers do not normally have access. However, the office is frequently left unoccupied when guards are busy elsewhere in the cell area.

It was evident that the photographs and documents were too small to be discernible from the open counter at the front of the office, or even from the doorway. Given that the bulletin board is

mounted on the same wall as the door and counter, someone would have had to enter the office and approach it to read the details. The investigator was unable to determine who had seen the material.

The information has since been removed from the bulletin board and placed in one of the desks. The RCMP is drafting a policy to control the display of identifying information about detainees who are HIV-positive or who have developed AIDS.

The Commissioner considered it reasonable for the RCMP to inform guards about individuals who pose a risk to employees and other prisoners. He concluded that the display did not breach the *Act*. However, while the Commissioner remains concerned about organizations assembling inventories of people identified as HIV-positive, he appreciates the quick action of both AIDS organizations, and the RCMP's immediate response.

Doing the bureaucratic shuffle

The man looking for information about his participation in EIC job training programs in 1975 complained to the Commissioner when all he got was a run-around.

First he went to his local Canada Employment Centre where he was told that the department did not keep the information as far back as 1975. He consulted *Info Source* (the directory of government information holdings) which confirmed that the training files were indeed kept for 25 years. Reassured he went to EIC's Toronto regional office and tried once again.

The regional office referred him back to his local CEC who repeated that the information did not exist. This time his request was referred to the National Archives.

During the shuffle, the complainant was given several inconsistent explanations. He was told the material was kept for only two

years, then seven years. The *Info Source* listing describes the retention period of one bank as indefinite; the second as two years for paper and 25 years for machine readable records.

The first thing the investigator needed to establish was just how long EIC kept the information in the two banks. Officials explained that the information is indeed kept for two years in individual Canada Employment centres, then it is transferred to a departmental archive where it is kept for a further five years. The information is then destroyed. Only statistical and program evaluation material (not personal information) is transferred to computer tapes and kept for 25 years.

The Commissioner concluded that the information had not been improperly destroyed and that complaint was not well-founded. However, he was concerned about the confusion, the repeated re-routing of the complainant's request and the inconsistent explanations about why the information did not exist. He asked EIC to clarify its explanation of the retention periods in *Info Source*—the tool on which the public depends to gain access to their records.

Improper Collection of Medical Information

An employee of the St. Lawrence Seaway Authority (SLSA) complained to the Commissioner when he was refused pay for two days sick leave because he would not disclose the nature of his illness to his supervisor.

SLSA policy required all employees claiming sick leave to supply the medical details on the "Application for Leave" form. The information was then reviewed by the employee's immediate supervisor who determined whether the condition warranted payment of sick leave.

SLSA staff argued that supervisors must collect and assess the information because occupational health and safety rules require

SLSA to ensure returning employees will not endanger themselves or colleagues. They also argued that collecting the medical details kept employees honest and was an important factor in controlling absenteeism and reducing costs.

The Privacy Commissioner recognizes that employers have a right to satisfy themselves that an employee's absence is justified, and there may be occasions when it will need to collect medical information from employees before endorsing sick leave requests. However, he does not agree with unqualified personnel collecting and assessing medical information. The Commissioner considered the complaint well-founded since the right to collect medical details to assess an employee's fitness should be reserved only for a qualified medical practitioner.

SLSA officials responded by changing their sick leave collection procedures, in place since the 1960s. The nature of illness is no longer disclosed to supervisors. When needed, it is collected and reviewed only by qualified medical practitioners.

Locator information unnecessary

An inmate asked for access to his Offender Grievance Files at Correctional Services Canada (CSC). He complained to the Commissioner when CSC refused to process the request, claiming he had not provided them with all the locator information needed to find the files.

The investigator found that every CSC institution keeps either a computer or manual log of all grievances submitted by inmates in their institution. Any CSC institution could easily identify and locate an inmate's grievance file in that institution just by using the inmate's name. The additional locator information was not necessary. CSC admitted that it could retrieve the file using the name and agreed to change its requirements for access to this information.

The complaint was well-founded.

Public interest release prompts complaint

Last year the Office reported receiving a complaint against the Privy Council Office (PCO) following its disclosure of personal information about two members to their professional body.

The case illustrates the limitations on the Commissioner's powers and the individual's rights in these "public interest" disclosures. It also demonstrates why staff examine the disclosure notices: the Commissioner must not have pre-judged the release and be prevented from ruling on a subsequent complaint.

The material was produced during a federal commission of inquiry. The commission report recommended the professional body review its members' conduct and PCO (the custodian) agreed to the body's subsequent request for the records. PCO advised the Commissioner, arguing there was a public interest in the body maintaining its professional standards.

The Office recommended notifying the two members (and their clients whose information would also be disclosed as evidence) and PCO agreed. One of the two then complained to the Commissioner.

The Commissioner reviewed PCO's procedure, the inquiry commission's recommendation, the material released and the powers of the professional body to compel evidence and conduct investigations.

He concluded that the disclosure did not violate the *Privacy Act*. He also pointed out that the professional body's powers were sufficient to compel PCO to produce the material under another provision of the *Act*.

Access to consent of “other parent”

An estranged husband asked External Affairs’ passport office to provide him with a copy of his declaration, signature and consent contained in his wife’s application to include their children on her passport.

The passport office replied that since the application belonged to his wife, he would need her authorization to obtain a copy.

The investigator examined the material and disagreed, pointing out that the information belonged to the husband since it refers to the “other parent”, not the parent completing the passport application. The passport office was unconvinced and very reluctant. After much debate, it finally released the disputed information. The Commissioner considered the complaint well-founded and resolved.

Parole Board fine tunes process

The National Parole Board often has to consult other organizations such as provincial government agencies or police forces before completing an access request. In one case, the Board wrote to several organizations asking for consent to release information they had provided about the applicant.

All but one responded in time for the board to process the request within the required 60 days. However, the PEI Crown Prosecutor did not respond to several letters. After many months, the board finally reached him and he agreed to release the information.

Given the time it took to get a response (and the well-founded complaint to the Commissioner), NPB decided to change its consultation process. Consultation letters now state that if the board does not receive a reply by a specific date, it will process the information in accordance with the federal *Privacy Act*. The onus has now shifted; an organization must respond quickly if it

wants to refuse to disclose information. And applicants are not kept waiting needlessly for months.

Questionnaires need own bank

Several Employment and Immigration Canada (EIC) employees complained through their union that a questionnaire collecting personal information for the department's Human Resource Inventory Program (HRPIP) violated their rights under the *Privacy Act*.

They complained that they had not been told the purpose for the collection. They also alleged that managers had ordered them to complete the supposedly voluntary questionnaire, requiring them to consent to all subsequent uses and disclosures of the information. They argued that this was a de facto avoidance of the use and disclosure provisions of the *Privacy Act*. Finally, they complained that the information being collected was not described in *Info Source*, as required by the *Privacy Act*.

EIC was sensitive to the employees' privacy concerns. Although it had tried to ensure full compliance with the *Privacy Act* in carrying out the project, some details had to be addressed.

The investigator found no evidence to substantiate the claim that employees had been ordered to complete the questionnaire. Although the language was not entirely clear, on second reading it was possible to determine that completing it was voluntary. However, EIC officials agreed to clarify the opening statement.

It was true that the collected information was not described in *Info Source*. EIC officials explained that all the separate pieces of information were described in the various standard employee banks, so it was unnecessary to develop a new bank. The Commissioner disagreed, viewing this as a distinct bank of personal information collected for a specific purpose.

Since many departments have similar programs (and there is no standard employee bank for this information), the Commissioner decided to accept EIC's explanation, close the complaint file, and work with Treasury Board to develop a new government-wide standard bank for these records.

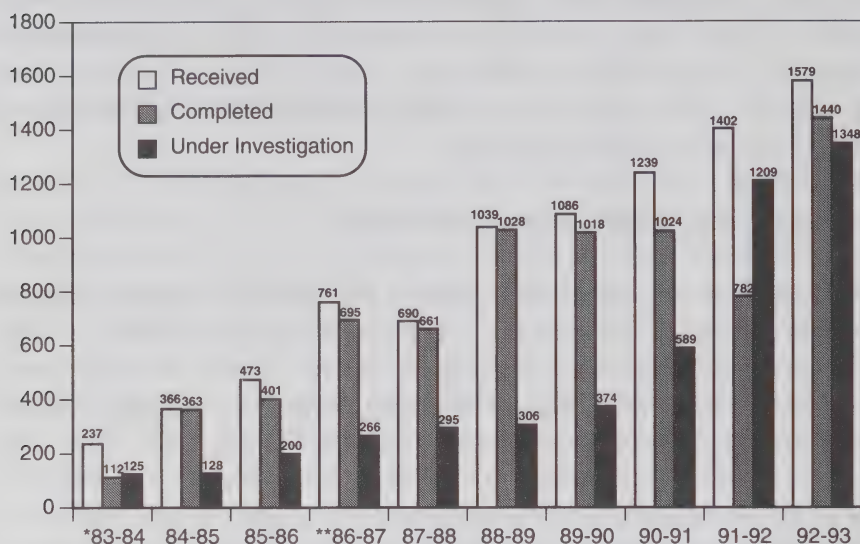
Inmates receive each other's records

Two inmates in a federal penitentiary complained that the personal information of each inmate had been improperly disclosed to the other. Both had requested their own records but when they were delivered, each envelope was found to contain the others' files, despite being properly addressed.

Staff at the institution confirmed that the incident happened substantially as reported. However, the files had arrived at the institution in sealed envelopes so the investigation focused on the privacy coordinator's office in headquarters where the envelopes had originated.

The investigator confirmed that controls are in place to prevent such incidents. However, the sheer volume of files handled by CSC headquarters, combined with shortages of trained staff to cope with that volume, made it almost inevitable that a mistake would happen. The Commissioner concluded that the two complaints were well-founded but made no recommendation that CSC institute further controls. The mix-up was probably attributable to human error.

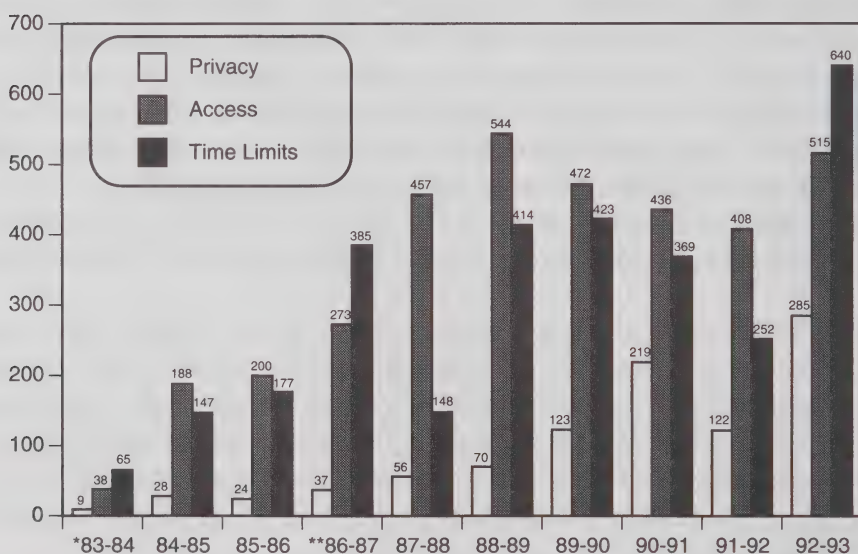
Completed Complaints 1983-93



* 9 Months

** Revised counting method

Completed Complaints and Grounds 1983-93



* 9 Months

** Revised counting method

Top Ten Departments by Complaints Received

		Grounds		
Institution	TOTAL	Access	Time Limits	Other
Correctional Service Canada	417	161	215	41
Revenue Canada - Taxation	158	34	111	13
Employment and Immigration Canada	133	51	51	31
Health and Welfare Canada	132	90	28	14
Canada Post Corporation	119	54	22	43
Canadian Security Intelligence Service	95	86	9	0
Royal Canadian Mounted Police	92	62	12	18
Revenue Canada - Customs & Excise	92	24	60	8
National Defence	72	34	22	16
Transport Canada	48	40	4	4
OTHER	221	107	68	46
TOTAL		743	602	234

Completed Complaints by Grounds and Results

		Disposition				
Grounds		Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued	TOTAL
Access		10	114	351	40	515
	Access	9	96	334	38	477
	Correction/Notation	1	4	14	2	21
	Index	0	14	0	0	14
	Language	0	0	3	0	3
Privacy		28	25	204	28	285
	Collection	2	4	95	10	111
	Retention & Disposal	6	5	4	0	15
	Use & Disclosure	20	16	105	18	159
Time Limits		403	0	202	35	640
	Time Limits	339	0	93	30	462
	Extension Notice	64	0	109	5	178
	TOTAL	441	139	757	103	1,440

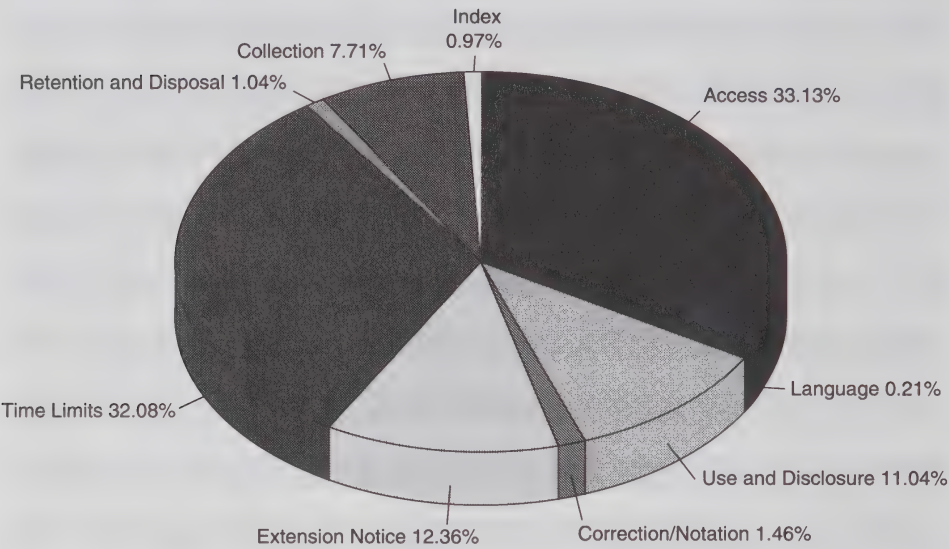
Completed Complaints by Department and Result

Department	TOTAL	Disposition			
		Well-founded	Well-founded; Resolved	Not Well-founded	Discon- tinued
Agriculture Canada	11		1	9	1
Canada Labour Relations Board	1			1	
Canada Mortgage and Housing Corp.	2			2	
Canada Post Corporation	73	30	10	30	3
Canadian Security Intelligence Service	89		2	85	2
Communications, Department of	8	8			
Correctional Service Canada	388	161	40	142	45
Employment and Immigration Canada	147	26	33	74	14
Energy, Mines and Resources Canada	8		6	2	
Environment Canada	9	5	2	2	
External Affairs Canada	14	1	3	10	
Farm Credit Corporation Canada	2		2		
Fisheries and Oceans	2		1		1
Health and Welfare Canada	37	19	5	10	3
Immigration and Refugee Board	36		2	34	
Indian and Northern Affairs Canada	3			3	
Justice Canada, Department of	20	5	3	12	
Labour Canada	4	1		3	
National Archives of Canada	45	21		24	
National Defence	112	26	6	77	3

Completed Complaints by Department and Result

Department	TOTAL	Disposition			
		Well-founded	Well-founded; Resolved	Not Well-founded	Discon- tinued
National Film Board	2			2	
National Parole Board	22	2	1	15	
Pension Appeals Board Canada	3	1	1	1	
Privy Council Office	19	2	2	15	
Public Service Commission of Canada	6		1	3	2
Public Service Staff Relations Board	1				1
Public Works Canada	1			1	
RCMP Public Complaints Commission	3	1		1	1
Revenue Canada, Customs and Excise	53	38	3	12	
Revenue Canada, Taxation	172	86	4	75	7
Royal Canadian Mint	4				4
Royal Canadian Mounted Police	60		2	53	5
Secretary of State of Canada	13	4	2	6	1
Solicitor General Canada	11		1	10	
St. Lawrence Seaway, The	1		1		
Statistics Canada	7			3	4
Supply and Services Canada	1				1
Transport Canada	30	2	5	22	1
Transportation Safety Board of Canada	1			1	
Treasury Board of Canada Secretariat	7			7	
Veterans Affairs Canada	12	2		10	
TOTAL	1440	441	139	757	103

Complaints Completed by Grounds 1992-93



Assessing Compliance

This has been a year of change and adjustment for the Compliance Directorate. In addition to a full workload (nine compliance audits, two special investigations, 12 follow-up audits and a study of information technology from a privacy perspective), the unit became the focal point for an Office-wide operational renewal.

The directorate was originally envisaged as an audit unit which would conduct systematic independent reviews of the 160-odd federal institutions subject to the *Privacy Act*. The workload this generated, combined with the need to examine emerging privacy issues, have proved simply beyond the limited resources available. However, the Office is unwilling to abandon this goal and simply react to complaints.

To meet this challenge, the operations and structure of the directorate have been redesigned. The result is a fresh approach to audit selection (who we audit), audit scoping (what we look at) and methodology (how we investigate). Investigators are shifting emphasis away from physical security and information bank descriptions. They now give more attention to determining whether agencies are collecting only personal information that meets operational requirements, and properly using, sharing and disclosing information. These changes should enhance our ability to investigate privacy issues and reinforce our ability to inform Parliament on privacy matters.

Special Investigations

This year the Compliance Directorate completed two special investigations of potential violations of the *Privacy Act*.

Computer stolen from Veterans Affairs

Last year's annual report reported the theft of a portable computer from an office of Veterans Affairs (VA). Again this year VA

reported a computer containing personal information had been stolen from an employee's home. The employee had the authority to use the computer at home and had taken reasonable measures to secure it and the information it contained. Since our last report, VA has improved security measures to protect personal information stored in portable computers. As a result, the Commissioner decided not to notify the individuals concerned.

Personal computer use has increased dramatically in the public sector during the past decade and not just at the office. With the advent of work-at-home programs (telework) and light, powerful portables, personal information is leaving the workplace. However, our review of departmental practices this year reveals that departments are unable to account for the number, location and use of their personal computers.

It is passing curious that this latest theft at Veterans Affairs is only the second ever reported to this office. Have other computers gone astray but departments either do not have the proper controls in place to identify the losses or to report the incidents to our office?

Personal information found in surplus file cabinets

The office received a call that used filing cabinets being sold at a warehouse surplus store still contained personal documents. Only a remarkable coincidence led to the office hearing about the incident—the caller once worked for the Privacy Commissioner's office. Investigators retrieved the documents and confirmed that they had originated in two federal departments.

The first group of documents included more than a dozen Transport Canada files, one of which was an employee travel expense claim file (the rest were not personal). This file contained substantial detail from the employee's transfer including utility bills, mortgage documents and even a cancelled cheque with his bank account number.

The second group originated with Health and Welfare Canada and was far more sensitive. It contained approximately 370 index cards documenting the lab tests undergone by each individual (but not the results). Investigators immediately notified the two departments and returned the documents.

Both departments investigated and reported back that they have procedures for ensuring that all documents are removed from any equipment declared surplus. Both acknowledged that they had been lax and began briefing staff and improving physical security. Although this office has no evidence to suggest that personal information is regularly being left in equipment declared surplus, the company reported it frequently finds documents in old cabinets.

The incident, while embarrassing for the departments involved, should remind all federal institutions to review their procedures and communicate them to staff.

Audits of Institutions

The Directorate completed audits of nine institutions this year: the Canadian International Trade Tribunal, Elections Canada, the National Library of Canada, the Canadian Transportation Accident Investigation and Safety Board, National Research Council Canada, Veterans Affairs Canada, Bureau of Pensions Advocates Canada, the Canadian Pension Commission and Veterans Appeal Board Canada.

The audit of Labour Canada, begun in 1992, is nearing completion. In addition, Indian and Northern Affairs Canada and the Bank of Canada are currently conducting their own internal privacy audits. Privacy staff will review the results of these audits in the coming year.

Common themes

One summary observation from this year's audits is the improved information management practices and better handling of personal information. This is particularly true in the area of information security and data maintenance. Despite this, audits continue to reveal a general lack of understanding of the *Privacy Act* and the role of this Office, particularly at the operational level.

We found several broad areas of concern during our audits.

Contracting out

Budget cuts and staffing freezes are causing more federal government institutions to contract to the private sector work involving personal information. Prime targets are Employee Assistance Programs, management consulting, computer programming and, in some cases, the day-to-day functioning of entire programs. Our audits continue to reveal that many contracts do not require contractors to comply with the *Privacy Act* and its code of fair information practices. Where investigators did find provisions about handling personal information in contracts, they were so general as to render them virtually ineffective for privacy protection.

Retention and disposal

Investigators continue to find instances of institutions not applying retention and disposal schedules and even of not developing these schedules. Retaining personal information beyond its approved period could harm an individual should staff make decisions about the person on the basis of invalid or out-of-date information.

***Info Source* descriptions**

In six of the nine institutions audited, investigators found information holdings that were not described in the *Info Source* directory or whose descriptions were incomplete or inaccurate. Since the right of access to personal information is one of the cornerstones of the *Act*, accurate descriptions of all personal information holdings are critical.

Access to personnel files

In most institutions audited, managers and supervisors can get access to the complete personnel files of their employees. This provides them access to sensitive personal information beyond their operational needs. This could include information such as divorce documents, support payments and designation of beneficiaries.

Regular readers of these reports will find many of these findings depressingly familiar; evidence the need to educate public servants.

Some Specific Observations

Office of the Chief Electoral Officer

This audit identified two key findings concerning the release of personal information from electoral lists. In the first case, investigators found that information was frequently being released under section 8(2)(m) of the *Privacy Act* to third parties (see Notifying the Commissioner). These disclosures were mainly to individuals to help confirm that they met residency requirements for pension or other legal claims.

However, the electoral office had never notified the Privacy Commissioner of these releases as the *Act* requires. When

investigators pointed this out, electoral staff agreed to notify the Commissioner in future.

The second finding concerned the electoral office's sharing of information from the federal electors list with municipalities to help them prepare for local elections. This disclosure did not appear to be a consistent use and electoral office staff agreed to either stop the practice or conclude formal agreements with individual municipalities to share this information and describe the new use in *Info Source*.

Veterans Affairs Canada

Veterans Affairs is an excellent example of an institution that complies with the *Privacy Act* and the code of fair information practices. Their commitment to training staff in privacy matters is encouraging and greatly facilitates proper management of personal information in the department.

A contract with Atlantic Blue Cross covering the administration of the Treatment Accounts Processing System, reviewed during the audit, could serve as a model for other departments that administer similar programs. Investigators also noted that privacy concerns are automatically considered in the design of the department's EDP systems.

One concern meriting specific mention concerns disposal of documents in the paper recycling bins. Like most departments, Veterans Affairs has an active paper recycling program. Despite instructions to the contrary, periodic inspections by VA security staff (and a sampling by the audit team) revealed personal information in the bins.

Following Up

To support this year's retrospective, investigators reviewed the outcome of several privacy compliance audits and complaints investigations conducted between 1984 and December 1989.

In order to determine whether departments had acted on the Office's recommendations, staff selected 20 audits and 116 recommendations stemming from complaint investigations.

Twelve institutions were examined in the past year: Agriculture Canada, Canada Post Corporation, Correctional Services Canada, Environment Canada, Fisheries and Oceans, Health and Welfare Canada, International Development Research Centre, Solicitor General Canada (Ministry Secretariat), Pension Appeals Board, Public Service Staff Relations Board, Supply and Services Canada and Transport Canada.

Investigators found about 74 per cent of all audit recommendations had been implemented, 16 per cent were partially completed or underway and the remaining 10 per cent had not been addressed.

Summary Observations

Overall, departments have responded positively to the Office's recommendations. Many recommendations have led to departments developing new policies and procedures at the corporate level. Unfortunately, this has not led to similar adjustments in the programs or regions. The reverse is also true; field offices have changed their practices to reflect the audit findings despite the absence of a change in corporate policy.

In general, investigators observed an overall improvement in attitude towards privacy. Government staff (particularly at the working level) are more aware of privacy concerns yet there is still minimal knowledge of the *Act* and its impact on federal

government operations. There is also little understanding of the role and functions of this Office.

These follow-ups also identified the difficulty experienced by some institutions in responding to recommendations involving the retention and disposal of personal information. Employee and client personal information are sometimes retained well beyond approved retention schedules and some schedules have not been approved at all. Departments cited budget constraints and delays at National Archives Canada as the cause.

Highlights by Institution

Agriculture Canada has acted on about half of the recommendations made in the Office's 1988 audit. Agriculture's treatment of personnel files is uneven; regional supervisors in some locations now have access only to relevant employee personal documents as recommended. However, in other locations, they see the entire employee record. Investigators found that 40 per cent of personnel files examined contained outdated employee performance appraisals and one general personnel file included a complete human rights investigation report containing very sensitive personal information.

Canada Post Corporation has acted on many of the recommendations from the 1988 compliance audit and follow-up from individual complaints. Investigators noted improved information bank descriptions, data security and policy development. However, they also found that regions were inconsistent in implementing some of the changes. For example, supervisors' access to employee files has been restricted at headquarters by splitting the files, removing third party information and fingerprints. Unfortunately, this has not been completed in most regional offices visited.

Correctional Service Canada has addressed many of the audit recommendations concerning access to personal information and

improved listings in *Info Source*. In addition, investigators reviewed several complaint investigations concerning disclosure of inmate personal information and confirmed that the recommended controls are now in place.

Environment Canada has not responded adequately to many of the Privacy Commissioner's recommendations. In fact, the Commissioner has not received a formal response to the 1988 audit report. Staff blamed centralization, decentralization and staff changes in the ATIP section for not completing the recommendations. The review found that some locations acted independently to improve protection of personal information and staff awareness. However, the corporate response has been disappointing.

Fisheries and Oceans was the first institution audited by the Office in 1985, serving as a test run for new auditors. Fisheries has complied with recommendations to stop collecting the social insurance number on fishing applications and cease publishing the Fishing Licence Directory containing personal information. However, the department continues maintaining indefinitely the personal records in the Atlantic Commercial Fishing Licence Database (PU-010) formerly Commercial Fishermen's and Vessel Registration bank.

Health and Welfare Canada has amended most of their personal information bank descriptions as recommended in the 1990 audit. The department has had less success disposing of outdated personal information at national headquarters and in one of the regions surveyed.

International Development Research Centre has dealt with most of the audit recommendations and is improving its protection of personal information while negotiating with National Archives Canada for an approved retention and disposal schedule.

Solicitor General Canada (SGC) has acted on most of the eight recommendations for improvement. Its request for an approved retention and disposal schedule from National Archives Canada is still outstanding. Although SGC has not purged staff personal records as recommended, its new automated Resource Management Information System (RMIS) will address this concern.

Supply and Services Canada responded positively to most of the concerns identified, restricting supervisors' access to employee personal records and registering all its personal information holdings in *Info Source*.

Transport Canada has responded to about 70 per cent of the recommendations made in the 1988 audit. Transport must be commended for its disposal of duplicate records containing highly sensitive personal information. However, the department has not yet amended the bank descriptions of its Aviation Licensing Database bank and Vehicle, Ship, Boat and Aircraft Accident bank. In addition, medical examination reports remain part of the Aviation Licensing Database rather than in the medical files, as recommended.

Both the **Pension Appeals Board** and **Public Service Staff Relations Board** have dealt with all our audit recommendations, resulting in proper identification of personal information holdings, better protection of information and an increased privacy awareness.

It's 1993 – Do you know where your information is?

Governments have always been massive collectors of personal data—but the growth of social programs and demand for government services, coupled with governments' vast technical ability to collect, manipulate and share information, make it vital for Canadians to know what governments know about them.

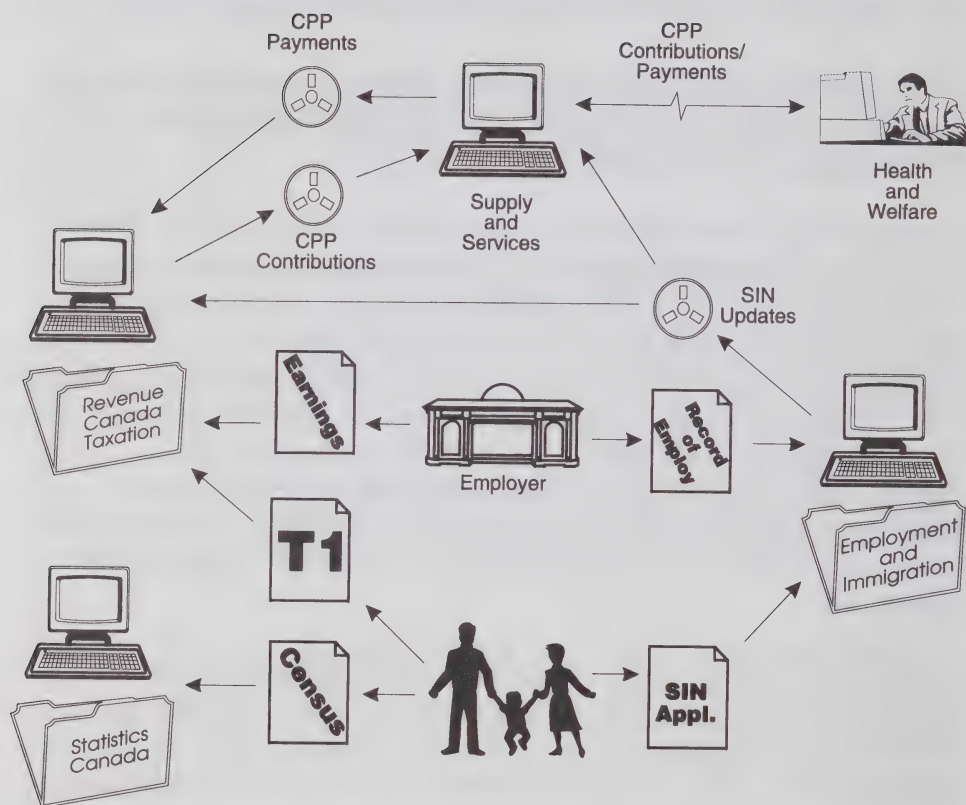
What personal data does the federal government hold? Although far from complete, most readers will recognize themselves somewhere in the following.

A key group of departments holds financial information on most Canadians. **Revenue Canada, Taxation** collects individual tax returns (approximately 17.5 million tax forms) which can contain everything from bank account numbers and charitable contributions to alimony payments and physical disabilities. **Health and Welfare Canada** manages the Canada Pension Plan (CPP) and Old Age Security programs, recording earnings and contributions. **Employment and Immigration** controls the Unemployment Insurance program which includes earnings, work history, benefits paid, and the Social Insurance Number (SIN) master list.

These main departments share information among themselves, primarily for financial checks and balances. For example, each year Revenue Canada gives Health and Welfare (through Supply and Services' computers) information on individuals' contributions to CPP, while Health and Welfare tells Revenue Canada about the CPP payments they make to individuals.

Chart 1 shows how the government collects some of its information from individuals and transfers it to other agencies.

Chart 1: Key Transfers of Personal Information in the Federal Government



Statistics Canada holds information about more Canadians (27.3 million) than any other agency, most of it drawn from the census. Everyone provides basic personal data, as well as their marital status, language, whether they own or rent their housing and who pays the household bills. One in five households provide more details, including ethnic origin, religion, physical and mental limitations, employment and income. Although this information is very personal, Statistics Canada uses it only for statistical purposes. Individuals' names are not entered into the computer (but the paper copies are kept).

Statistics Canada also conducts surveys such as those on consumer finances, health and work history. As well, the agency maintains long term databases on cancer and tuberculosis patients, dental hygienists, registered nurses and elementary and secondary school teachers.

Other agencies gather data from operational programs dealing with immigrants, native peoples, homeowners, Canada Savings Bonds purchasers, students, farmers, people who have changed addresses, and criminals. Some people's dealings with the government necessarily mean providing more details. For example:

- **Immigrants and Refugees**

Some 6,670,000 individuals have immigrated to Canada since the Second World War. Their files can contain information about education, work history, financial situation, physical and mental health, social and political involvements, criminal activities and family situation. As well, the government collects data about the immigrant's sponsors or hosts.

- **Native Peoples**

The government has a master index of approximately 530,000 registered status Indians, as well as paylists (including family members) for those receiving treaty payments. There are also nominal roles of students living on reserves, attendance records

and grades of those attending federal schools and case files of reserve children and families who receive various social services. As well, there are trust fund accounts, a land registry, small business loan funds and artist and prospectors' programs containing a range of personal and financial information.

- **Pensioners**

Pensioners' information falls into both financial and medical categories. There are Canada Pension Plan, Guaranteed Income Supplement and Spouse's Allowances files, all containing earnings and payments information. The Old Age Security Program alone has approximately 3,250,000 accounts. Pensioners receiving disability pensions also supplied detailed medical information to support their applications.

Veterans Affairs also maintains 550,000 accounts for veterans' pensions and benefits. These files can contain sensitive medical information, including complete medical and drug histories on patients in veterans' hospitals. And since some veterans programs impose a means test to determine benefits, some files contain financial information.

- **Armed Forces Members**

The dictates of their profession mean government has substantial information on current and former armed forces members. All members provide fingerprints, undergo security assessments and medical examinations. Since the forces provide members with ongoing medical care, there are detailed medical and dental files, and occasionally hospital reports. Inevitably members have training and education files, the latter particularly if the member attended a military college. There will also be personnel records, including performance evaluations, awards records, social services or disciplinary records. As well, the forces collect information on family members, particularly when the family lives on a military base or is posted with the member.

- **Inmates and Parolees**

Current inmates and parolees will have a wide range of personal data in the files of the RCMP, Correctional Services Canada and the National Parole Board. These can include criminal history and court records, medical and psychiatric reports, disciplinary measures imposed, intelligence reports, appraisals and recommendations from the parole board and victim impact statements.

Those who worry about Big Brother can be reassured—there is no one central file containing all these personal details. Some federal departments do share and match personal information but must respect policies and rules set out in various acts. Some federal agencies exchange information with provincial governments under formal agreements. For more details, see *Info Source*, the annual directory of the federal government's information holdings.

Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative, informatics and library services.

Finance

The Offices' total resources for the 1992-93 fiscal year were \$6,761,000 and 85 person-years, an increase of \$70,000 and three person-years over 1991-92. Personnel costs of \$5,351,077 and professional and special services expenditures of \$642,835 accounted for more than 88 per cent of expenditures. The remaining \$765,086 covered all other expenses.

The following are the Offices' expenditures for the period April 1, 1992 to March 31, 1993*

	Information	Privacy	Corporate Management	Total
Salaries	1,923,405	2,066,562	609,110	4,599,077
Employee Benefit Plan Contributions	306,000	342,000	104,000	752,000
Transportation and Communication	36,468	96,722	134,107	267,297
Information	26,954	69,435	2,242	98,631
Professional and Special Services	402,524	107,240	133,071	642,835
Rentals	9,275	66	12,107	21,448
Purchased Repair and Maintenance	14,758	790	25,511	41,059
Utilities, Materials and Supplies	18,887	11,762	36,841	67,490
Acquisition of Machinery and Equipment	86,709	47,680	130,192	264,581
Other Payments	2,434	1,475	671	4,580
TOTAL	2,827,414	2,743,732	1,187,852	6,758,998

* Expenditure figures do not incorporate final year-end adjustments reflected in the Offices' 1992-93 Public Accounts.

Personnel

The unit provided support for restructuring both Commissioners' offices and began implementing the government-wide classification simplification project. The Offices approved a new policy on leave and introduced an employee assistance program.

Administration

The branch reviewed office accommodation and made some improvements. In addition, it introduced new government initiatives to speed up the procurement of goods and services.

Informatics

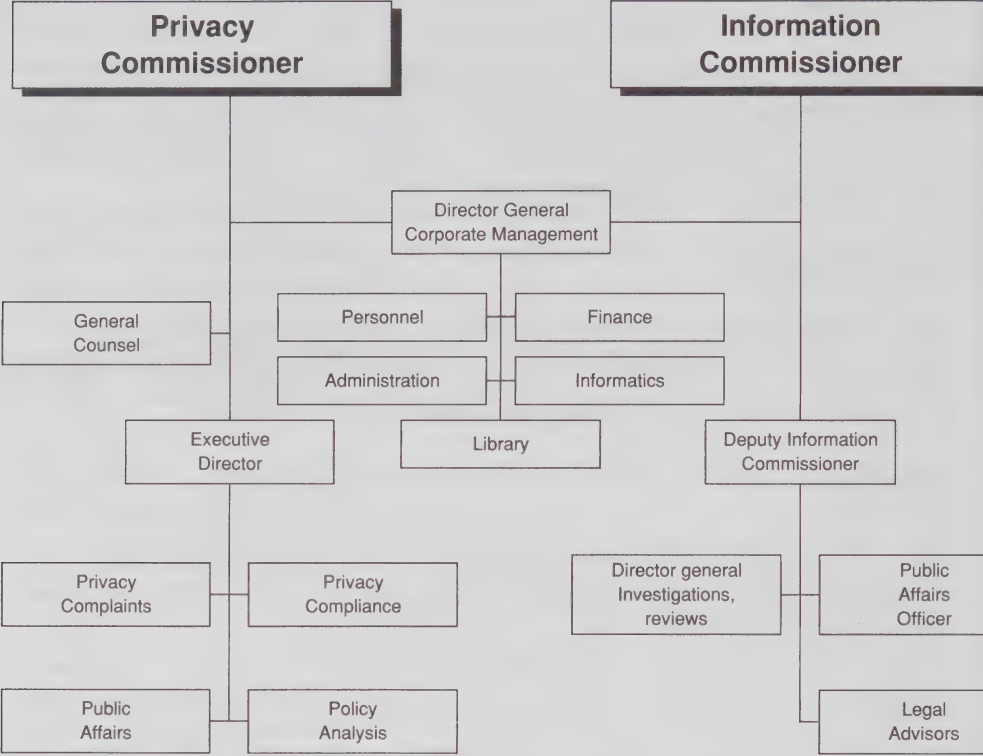
The Offices received funds to update the case management system and have established a local network and introduced new office automation tools.

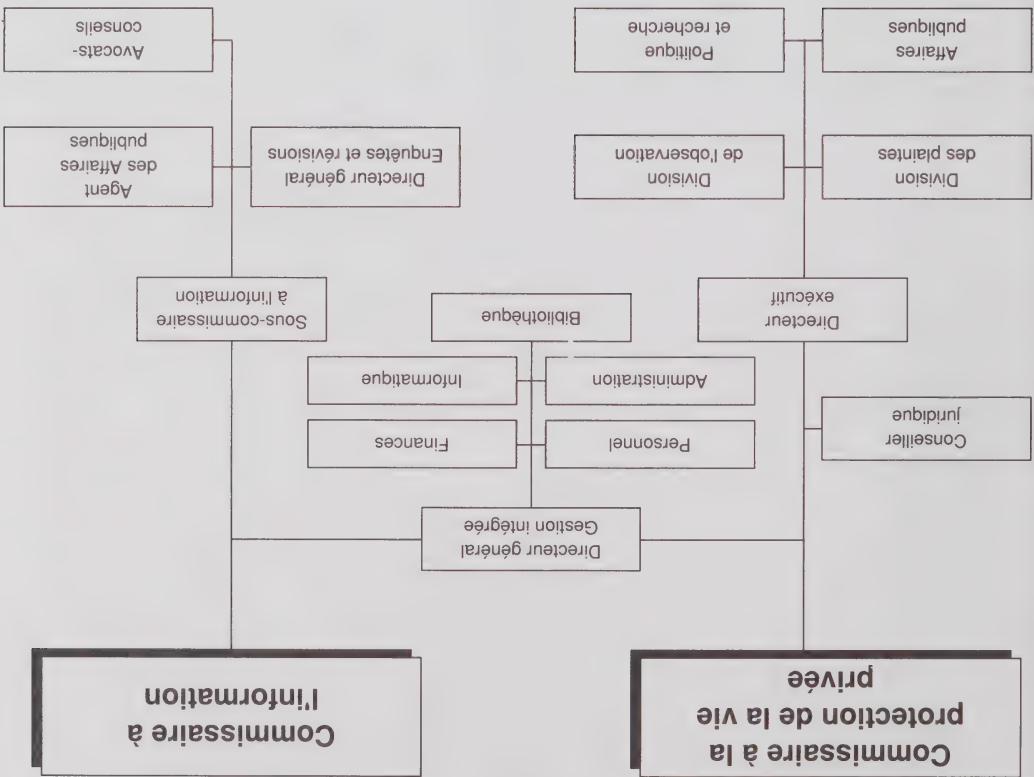
Library

The library provides interlibrary loan services, conducts manual and automated reference and research, and maintains subject-oriented media monitoring files. In addition to information on freedom of information, the right to privacy, data protection and the ombudsman function, the library has a special collection of Canadian and international ombudsmen's reports and departmental annual reports on the administration of the two acts. The library is open to the public.

During the year, the library acquired some 560 new publications and answered 1006 reference questions.

Organization Chart





Personnel

Les services du personnel ont apporté leur appui à la restructuration des deux commissariats et ont commencé la réalisation du projet de simplification de la classification, qui touche l'ensemble de la fonction publique. Les commissariats ont approuvé une nouvelle politique en matière de congés et instauré un programme d'aide aux employés.

Administration

Les locaux ont fait l'objet d'une étude, et des améliorations y ont été apportées. De plus, les nouvelles initiatives du gouvernement visant à accélérer les achats de biens et services ont été mises en place.

Informatique

Les commissariats ont reçu des fonds pour actualiser leur système de gestion des cas. Un réseau local a été créé et de nouveaux outils informatiques ont été installés.

Bibliothèque

Les services de la bibliothèque sont : les prêts entre bibliothèques, la documentation et les recherches manuelles et automatisées et la tenue de dossiers thématiques de coupures de presse. Outre les documents sur l'accès à l'information, la protection des renseignements personnels et la fonction d'ombudsman, la bibliothèque contient une collection spéciale de rapports d'ombudsmans canadiens et étrangers et de rapports annuels sur l'application des deux lois. Elle est ouverte au public.

Au cours de l'année, la bibliothèque a fait l'acquisition de quelque 560 nouvelles publications et son personnel a répondu à 1 006 questions à caractère documentaire.

La Gestion intégrée assure à la fois au Commissariat à l'information et au Commissariat à la protection de la vie privée des services en matière de finances, de gestion du personnel, d'administration, d'informatique et de bibliothèque.

Finances

Pour l'exercice financier 1992-1993, les ressources des commissariats ont totalisé 6 761 000 \$ et 82 années-personnes, soit une augmentation de 70 000 \$ par rapport à 1991-1992. Les dépenses au titre du personnel 5 351 077 \$ ainsi que les services professionnels et spéciaux 642 835 \$ représentent plus de 88 p. 100 des dépenses. Les 765 086 \$ qui restent ont servi à couvrir les autres frais.

Ci-dessous les dépenses des commissariats pour la période allant du 1^{er} avril 1992 au 31 mars 1993*

	Information	Vie privée	Gestion Intégrée	Total
Salaires	1 923 405	2 066 562	609 110	4 599 077
Contributions aux régimes d'avantages sociaux des employés	306 000	342 000	104 000	752 000
Transports et communications	36 468	96 722	134 107	267 297
Information	26 954	69 435	2 242	98 631
Services professionnels et spéciaux	402 524	107 240	133 071	642 835
Locations	9 275	66	12 107	21 448
Achats de services de réparation et d'entretien	14 758	790	25 511	41 059
Services publics, fournitures et approvisionnements	18 887	11 762	36 841	67 1
Acquisition de machines et d'équipement	86 709	47 680	130 192	264 581
Autres dépenses	2 434	1 475	671	4 1
TOTAL	2 827 414	2 743 732	1 187 852	6 758 998

* Les dépenses n'incluent pas les ajustements de fin d'année retelés dans la section des comptes publics 1992-1993 traitant des commissariats.

gouvernements provinciaux en vertu d'ententes officielles. Pour obtenir plus de détails, le lecteur consultera *Info Source*, le répertoire annuel des renseignements détenus par le gouvernement fédéral.

• **Membres des Forces armées**

En raison des impératifs de leur profession, le gouvernement possède beaucoup de renseignements sur les militaires, actuels ou anciens. Tous les militaires fournissent leurs empreintes digitales, passent une évaluation de la sécurité et subissent des examens médicaux. Puisque que les forces offrent à leurs membres des soins médicaux constants, il existe donc des dossiers médicaux et dentaires détaillés et, parfois, des dossiers d'hospitalisation. En outre, il existe nécessairement des dossiers sur la formation et les études surtout si, dans le dernier cas, le membre a fréquenté un collège militaire. On retrouve aussi des dossiers du personnel, dans lesquels sont versés les évaluations de rendement, les décorations, les dossiers de services sociaux ou des dossiers disciplinaires. De plus, les forces armées recueillent des renseignements sur les membres de la famille, surtout si la famille réside sur une base militaire ou se trouve sur les lieux d'affectation du militaire.

• **Détenus et libérés conditionnels**

La GRC, le Service correctionnel du Canada et la Commission nationale des libérations conditionnelles détiennent un vaste éventail de renseignements personnels sur les détenus et les libérés conditionnels. On trouve des dossiers sur les antécédents criminels, des dossiers judiciaires, des rapports médicaux et psychiatriques, des dossiers sur les mesures disciplinaires, des rapports des services de renseignements, des dossiers sur les évaluations et les recommandations de la Commission des libérations conditionnelles et des déclarations de la victime.

Ceux qui craignent le Grand Frère peuvent se rassurer—il n'existe pas de fichier central contenant tous ces renseignements personnels. Des ministères fédéraux échangent et appartiennent les renseignements personnels, mais ils doivent respecter les politiques et les rôles énoncés dans les diverses lois. Certains organismes fédéraux échangent des renseignements avec des

• Autochtones

Le gouvernement détient un répertoire principal sur environ 530 000 Indiens de plein droit, de même que des listes de paye (qui portent aussi sur les membres de la famille) des bénéficiaires des paiements prévus par les traités. Il y a aussi des états nominatifs des élèves vivant sur les réserves, des fiches de présence, des notes d'élèves qui fréquentent des écoles fédérales et des dossiers sur des enfants et des familles des réserves qui reçoivent divers services sociaux. En outre, les comptes des fiduciaires, le registre des terres indiennes, les fonds de prêts aux petites entreprises et les programmes d'aide aux artistes et aux prospecteurs contiennent une vaste gamme de renseignements personnels et financiers.

• Retraites

Les renseignements sur les retraites sont d'ordre financier et médical. Il y a les dossiers du Régime de pensions du Canada, du Supplément de revenu garanti et du programme d'allocation au conjoint qui contiennent tous des renseignements sur les revenus et les prestations. Le programme de la sécurité de la vieillesse regroupe à lui seul environ 3 250 000 comptes. Les retraités qui reçoivent une pension d'invalidité ont dû également fournir des renseignements médicaux détaillés à l'appui de leur demande.

Le ministère des Anciens combattants maintient aussi 550 000 comptes sur les pensions et les prestations versées aux anciens combattants. Ces dossiers peuvent contenir des renseignements médicaux de nature délicate, y compris des antécédents médicaux complets et des antécédents sur les médicaments consommés relativement aux patients dans les hôpitaux des anciens combattants. Et depuis que des programmes destinés aux anciens combattants calculent les prestations en fonction des ressources, on retrouve dans certains dossiers des renseignements financiers.

Statistique Canada détient des renseignements sur plus de

Canadiens (27,3 millions) que tout autre organisme, surtout grâce au recensement. Chaque personne fournit des renseignements personnels de base et signale son état civil, sa langue, si elle est propriétaire ou locataire, et qui paie les factures du ménage. Un ménage sur cinq donne plus de détails, y compris l'origine ethnique, la religion, les handicaps physiques et mentaux, l'emploi et le revenu. Même si ces renseignements sont de nature très personnelle, Statistique Canada les utilise uniquement à des fins de statistique. Les noms des personnes ne sont pas versés dans l'ordinateur (mais les copies sur papier sont conservées).

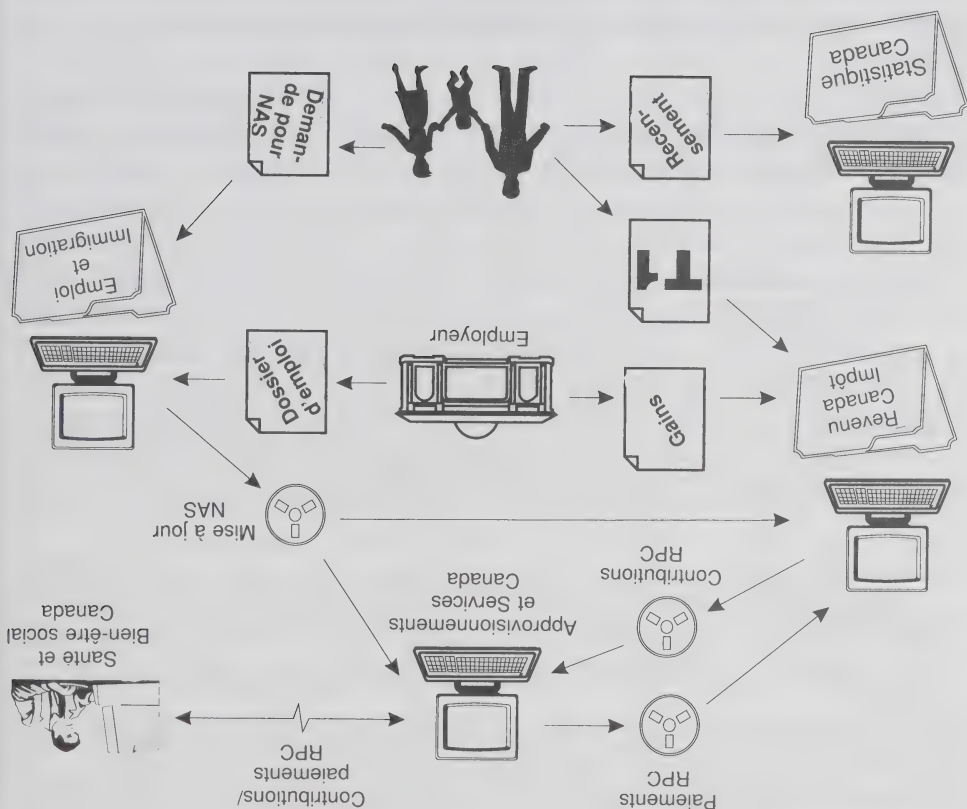
Statistique Canada mène souvent des études, par exemple sur la situation financière sur la santé et sur les antécédents de travail du consommateur. De même, il maintient des bases de données à long terme sur les patients atteints du cancer ou de tuberculose, les hygiénistes dentaires, les infirmières autorisées et les enseignants des écoles élémentaires et secondaires.

D'autres organismes recueillent des données provenant des programmes opérationnels relatifs aux immigrants, aux autochtones, aux propriétaires d'habitations, aux acheteurs des obligations d'épargne du Canada, aux étudiants, aux fermiers, aux personnes ayant déménagé et aux criminels. Les personnes traitant avec le gouvernement doivent nécessairement fournir plus de renseignements. En voici des exemples.

• Immigrants et réfugiés

Quelque 6 670 000 personnes ont immigré au Canada depuis la Seconde Guerre mondiale. Leurs dossiers peuvent contenir des renseignements sur leurs études, leurs antécédents de travail, leur situation financière, leur santé physique et mentale, leur participation dans des mouvements sociaux et politiques, leurs activités criminelles et leur situation familiale. De même, le gouvernement recueille des données sur ceux qui parrainent ou reçoivent un immigrant.

Tableau 1: Transferts principaux de renseignements
personnels au sein du gouvernement fédéral



En l'an 1993—Où sont vos renseignements?

Les gouvernements ont toujours recueilli des tonnes de renseignements personnels—mais en raison de la croissance des programmes sociaux, de la demande croissante en services gouvernementaux, ainsi que des vastes moyens techniques dont disposent les gouvernements pour recueillir, manipuler et échanger l'information, il est essentiel que les Canadiens connaissent ce que les gouvernements savent à leur sujet. Quels renseignements personnels le gouvernement fédéral détient-il? Quoique la description soit incomplète, la plupart des lecteurs se reconnaîtront dans l'un ou l'autre des aspects suivants.

Un groupe clé de ministères détient des renseignements financiers sur la plupart des Canadiens. **Revenu Canada** impôt recueille les déclarations d'impôt individuelles, soit environ 17,5 millions de formulaires, qui contiennent de tout (numéros de comptes de banque, dons charitables, paiements de pension alimentaire, handicaps physiques, etc.) **Santé et Bien-être social Canada** gère le Régime de pension du Canada et les programmes de la Sécurité de la vieillesse et il enregistre les revenus et les contributions. **Emploi et Immigration** contrôle le programme d'assurance-chômage qui comprend les gains, les antécédents de travail, les prestations payées et le fichier principal des numéros d'assurance sociale.

Ces principaux ministères échangeront l'information recueillie, surtout pour des vérifications financières et des soldes. Ainsi, chaque année, Revenu Canada donne accès à Santé et Bien-être social (grâce aux ordinateurs d'Approvisionnements et Services Canada) aux renseignements sur les contributions au Régime de pension du Canada; de son côté, Santé et Bien-être social Canada signale à Revenu Canada les paiements effectués par le Régime de pension du gouvernement.

demande d'un calendrier de conservation et de destruction approuvé. Bien que SGC n'a pas encore procédé à l'épuration des dossiers de ses employés comme il avait été recommandé, ce sera fait grâce à son nouveau système informatisé de gestion des ressources.

Approvisionnement et Services Canada a très bien réagi à la plupart des préoccupations cernées, restreignant l'accès des superviseurs aux dossiers des employés et inscrivant chacun de ses fichiers de renseignements personnels dans *Info Source*.

Transports Canada a mis en œuvre quelque 70 p. 100 des recommandations relatives à la vérification de 1988. Ce ministère mérite une bonne mention pour avoir éliminé les dossiers en double qui renfermaient des renseignements personnels de nature très délicate. Cependant, il n'a pas encore modifié les descriptions relatives à son fichier visant la délivrance des licences d'aviation et celui sur les accidents de véhicules, de navires, de bateaux et d'aéronefs. En outre, les rapports d'examen médical font encore partie du fichier visant la délivrance des licences d'aviation plutôt que d'être consignés aux dossiers médicaux, tel qu'il avait été recommandé.

La **Commission d'appel des pensions Canada** et la **Commission des relations de travail dans la Fonction publique** ont appliqué la totalité de nos recommandations de vérification, ce qui leur a permis d'améliorer la définition de leurs fichiers de renseignements personnels et la protection des renseignements personnels, ainsi que d'être davantage sensibilisés à la protection de la vie privée.

personnel du ministère blâme la centralisation, la décentralisation et le roulement du personnel de la section d'AI/RP pour la mise en œuvre incomplète des recommandations. Le suivi a permis de constater que certains bureaux ont pris l'initiative d'améliorer la protection des renseignements personnels et les connaissances des employés. Néanmoins, la réaction dans l'ensemble du ministère est décevante.

En 1985 **Pêches et Océans** a été le premier ministère à faire l'objet d'une vérification menée par le Commissariat, servant par le fait même de cas d'essai pour les nouveaux vérificateurs. Tel qu'il avait été recommandé, ce ministère a mis fin à la pratique de recueillir le numéro d'assurance sociale sur les demandes de permis de pêche et a cessé de publier le répertoire des permis de pêche qui renfermait des renseignements personnels. Le ministère continue toutefois de conserver indéfiniment les dossiers personnels de la banque de données sur l'immatriculation des bateaux et des permis de pêche commerciale.

Santé et Bien-être social Canada a modifié la plupart des descriptions de ses fichiers de renseignements personnels comme il avait été recommandé suite à la vérification de 1990. Le ministère n'a toutefois pas eu autant du succès au chapitre du retrait des renseignements personnels périmés qui sont encore conservés à l'administration centrale et dans l'une des régions étudiées.

Le Centre canadien de recherches pour le développement international a pris des mesures à l'égard de la plupart des recommandations issues de la vérification. Il fait des progrès sur le plan de la protection des renseignements personnels tout en négociant l'approbation d'un calendrier de conservation et de retrait avec les Archives nationales du Canada.

Le Solliciteur général Canada (SGC) a mis de l'avant la plupart des huit recommandations d'amélioration. Il attend toujours une réponse de la part des Archives nationales du Canada à sa

régionaux, les superviseurs n'ont maintenant accès qu'aux documents personnels pertinents des employés, tel qu'il avait été recommandé. Dans d'autres, cependant, il n'existe encore aucune restriction à cet égard. Les enquêteurs ont constaté que 40 p. 100 des dossiers d'employés examinés renfermaient des évaluations de rendement périmees, sans parler du dossier général de l'employé, lequel contenait un rapport complet d'enquête relative aux droits de la personne comportant des renseignements personnels de nature très délicats.

La Société canadienne des postes a mis en pratique un grand nombre des recommandations formulées à l'issue de la vérification de conformité de 1988 et du suivi de plaintes individuelles. Les enquêteurs ont constaté une amélioration sur les plans des descriptions relatives aux fichiers de renseignements, de la sécurité des données et de l'élaboration de politiques. Ils ont toutefois remarqué de l'incohérence dans la mise en œuvre de certaines des modifications par les régions. À l'administration centrale par exemple, l'accès aux dossiers d'employés par les superviseurs a été restreint en scindant les dossiers et en retirant l'information sur les tiers et les empreintes digitales. Malheureusement, cela n'a pas été fait dans la plupart des bureaux régionaux qui ont reçu la visite des enquêteurs.

Le Service correctionnel Canada a mis en œuvre de nombreuses recommandations concernant l'accès à des renseignements personnels, et l'amélioration des données publiées dans *Info Source*. De plus, les enquêteurs ont étudié plusieurs enquêtes menées à la suite de plaintes relatives à la divulgation de renseignements personnels de détenus et ils sont en mesure de confirmer que les mesures de contrôle recommandées ont été instaurées.

Environnement Canada n'a pas donné suite de façon satisfaisante à nombre des recommandations du Commissaire à la protection de la vie privée. De fait, ce dernier n'a pas reçu de réponse officielle à son rapport de vérification de 1988. Le

Observations générales

Dans l'ensemble, les ministères ont fait bon accueil aux recommandations du Commissariat. Nombre de ces dernières ont mené à l'élaboration de nouvelles politiques et procédures à l'échelle ministérielle. Malheureusement, cela n'a pas entraîné de redressements semblables au chapitre des programmes ou des régions. L'inverse est aussi vrai : des bureaux régionaux ont modifié leurs pratiques afin de tenir compte des résultats de nos vérifications, et cela même si aucune modification n'avait été apportée à la politique ministérielle.

Les enquêteurs ont remarqué une amélioration générale de l'attitude à l'égard de la protection des renseignements personnels. Les fonctionnaires (en particulier, au niveau opérationnel) sont plus conscients des préoccupations en matière de vie privée. Malgré tout, ils ont encore une connaissance très limitée de la Loi et de ses incidences sur le mode de fonctionnement du gouvernement fédéral et ils comprennent mal le rôle et les fonctions du Commissariat.

Le suivi a également fait ressortir que la mise en œuvre des recommandations touchant la conservation et le retrait des renseignements personnels ne va pas quelquefois sans difficulté au sein de certaines institutions. Ainsi, les renseignements personnels ayant trait aux employés et aux clients sont conservés bien plus longtemps que la période de conservation prescrite sur les calendriers, dont certains n'ont même jamais été approuvés. Selon les ministères, les compressions budgétaires et les délais aux Archives nationales du Canada en seraient la cause.

Faits saillants du suivi par institution

Agriculture Canada a répondu à environ la moitié des recommandations découlant de la vérification effectuée par le Commissariat en 1988. Au sein de ce ministère, les dossiers des employés sont traités de façon inégale. Dans certains bureaux

Suivi

interne et l'échantillon pris par l'équipe de vérification, il arrive que des documents renfermant des renseignements personnels soient jetés dans ces contenants, et cela malgré les consignes.

À l'appui de la rétrospective de cette année, les enquêteurs ont examiné plusieurs vérifications de conformité et plaintes relatives à la protection des renseignements personnels qui avaient été traitées entre 1984 et décembre 1989.

Le personnel a choisi 20 vérifications et 16 recommandations découlant d'enquêtes sur les plaintes afin de déterminer dans quelle mesure les ministères avaient donné suite aux recommandations du Commissariat.

Douze institutions ont été examinées au cours de l'année écoulée : Agriculture Canada, la Société canadienne des postes, Service correctionnel Canada, Environnement Canada, Pêches et Océans, Santé et Bien-être social Canada, le Centre canadien de recherches pour le développement international, Solliciteur général Canada (Secrétariat du Ministère), la Commission d'appel des pensions, la Commission des relations de travail dans la Fonction publique, Approvisionnement et Services Canada et Transports Canada.

Les enquêteurs ont constaté que 74 p. 100 de toutes les recommandations effectuées en rapport suite aux vérifications avaient été mises en œuvre, tandis que 16 p. 100 l'avaient été de façon partielle ou étaient en voie de l'être et que 10 p. 100 étaient restées lettre morte.

enquêteurs ont fait valoir ce point, le personnel a convenu de s'y conformer à l'avenir.

La deuxième constatation touchait la communication des renseignements des listes électorales fédérales aux municipalités en vue d'aider ces dernières à préparer les élections municipales. Une telle communication ne semblait pas conforme et le personnel de l'organisme s'est engagé à mettre fin à cette pratique ou à conclure des ententes formelles avec les différentes municipalités pour la communication de l'information et la description de la nouvelle utilisation de cette information dans *Info Source*.

Anciens Combattants Canada

Ce ministère est un bel exemple d'une institution qui respecte la *Loi sur la protection des renseignements personnels* et son code de pratiques équitables en matière d'information. Son engagement à l'égard de la formation de son personnel en matière de la protection de la vie privée est fort encourageant; il facilite en outre la bonne gestion des renseignements personnels au sein de ce ministère.

Le contrat conclu avec Atlantic Blue Cross et portant sur l'administration du Système de comptabilisation des traitements, lequel contrat a été examiné au cours de la vérification, pourrait servir de modèle à tous les ministères qui administrent des programmes semblables. Les enquêteurs ont aussi remarqué que les préoccupations en matière de protection des renseignements personnels faisaient partie intégrante de la conception des systèmes informatiques du ministère.

Il y a tout de même une préoccupation qui mérite d'être mentionnée au sujet des documents jetés dans les contenants de recyclage du papier. Comme la plupart des autres ministères, Anciens Combattants Canada s'est doté d'un programme actif de recyclage du papier. Malheureusement, comme l'ont révélé les inspections périodiques effectuées par le personnel de sécurité

Notre vérification a fait ressortir deux constatations principales à l'égard de la communication des renseignements personnels contenus dans les listes électorales. Premièrement, les enquêteurs ont constaté qu'il arrivait fréquemment que cette information soit communiquée à des tiers en vertu de l'alinéa 8 (2)m) de la *Loi sur la protection des renseignements personnels* (voir «Communications au Commissaire»). Ces communications ont surtout été faites à des personnes qui devaient confirmer qu'elles satisfaisaient aux critères de résidence pour des questions de pension ou autres réclamations légales.

Toutefois, l'organisme n'en avait jamais avisé le Commissaire à la protection de la vie privée comme l'exige la *Loi*. Lorsque les

Bureau du Directeur général des Elections

Quelques observations précises

Nos fidèles lecteurs ne manqueront pas de remarquer que ces constatations reviennent souvent. C'est la preuve qu'une meilleure sensibilisation des fonctionnaires s'impose.

Dans la plupart des institutions fédérales, les gestionnaires et les superviseurs ont accès à tous les documents contenus dans les dossiers de leurs employés et peuvent donc prendre connaissance de renseignements de nature délicate qui leur sont inutiles. Il peut s'agir, par exemple, de documents de divorce, de renseignements sur une pension alimentaire ou de désignations de bénéficiaires.

Nos fidèles lecteurs ne manqueront pas de remarquer que ces

Accès aux dossiers d'employés

l'une des pierres angulaires de la *Loi*, il est d'une importance capitale que tous les fonds de renseignements soient inscrits avec exactitude au répertoire.

Dans le cours de nos vérifications, nous avons cerné les points de préoccupation suivants.

Sous-traitance

Les compressions budgétaires et le gel de la dotation en personnel incitent un plus grand nombre d'institutions fédérales à confier au secteur privé du travail et, ce faisant, des renseignements personnels. Les principaux domaines visés sont les programmes d'aide aux employés, la consultation en gestion, la programmation informatique et, dans certain cas, l'exécution courante de programmes entiers. Comme nos vérifications continuent de le révéler, nombre d'ententes ne stipulent pas que les entrepreneurs sont tenus de se conformer à la *Loi sur la protection des renseignements personnels* et aux exigences qu'elle comporte en termes de pratiques équitables en matière d'information. Par ailleurs, là où existent de telles dispositions, celles-ci sont tellement vagues qu'elles n'assurent à peu près aucune protection des renseignements personnels visés.

Conservation et destruction

Les enquêteurs ont de nouveau constaté que certaines institutions ne suivent pas les calendriers de conservation et de destruction et qu'elles allaient même jusqu'à omettre de les établir. Le fait de conserver des renseignements personnels plus longtemps que la période prescrite peut être préjudiciable aux personnes visées, car il peut arriver que le personnel de l'organisme prenne des décisions qui les concernent sur la foi de renseignements erronés ou dérimés.

Descriptions du répertoire *Info Source*

Six des neuf institutions faisant l'objet d'une vérification détenaient des fonds de renseignements qui n'étaient pas inscrits au répertoire *Info Source*, ou dont la description était incomplète ou inexacte. Le droit d'accès aux renseignements personnels étant

qu'elle trouvait fréquemment des documents dans de vieux classeurs.

L'incident, bien qu'embarrassant pour les ministères touchés, devrait inciter les diverses institutions fédérales à examiner leurs lignes directrices et à les communiquer à leur personnel.

Vérifications de conformité

La Direction a mené des vérifications dans neuf institutions au cours de l'exercice, soit le Tribunal canadien du commerce extérieur, Elections Canada, la Bibliothèque nationale du Canada, le Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports, le Conseil national de recherches du Canada, Anciens Combattants Canada, le Bureau des services juridiques des pensions Canada, la Commission canadienne des pensions et le Tribunal d'appel des anciens combattants Canada.

La vérification de Travail Canada, entreprise en 1992, est presque terminée. Par ailleurs, Affaires indiennes et du Nord Canada et la Banque du Canada procèdent actuellement à leur propre vérification interne de conformité à la Loi. Le personnel du Commissariat étudiera les résultats de ces vérifications au cours du prochain exercice.

Thèmes communs

L'observation générale qui se dégage des vérifications effectuées cette année est qu'il y a eu une amélioration au chapitre des pratiques de gestion de l'information et du traitement des renseignements personnels, et tout particulièrement en ce qui a trait à la sécurité de l'information et à la gestion des données. Malgré cela, les vérifications continuent de montrer que la Loi sur la protection des renseignements personnels et le rôle du Commissariat sont mal compris en général, surtout sur le plan opérationnel.

Renseignements personnels oubliés dans des classeurs revendus

Le Commissariat a reçu un appel indiquant que des classeurs vendus à un magasin de matériel d'occasion contenaient encore des documents personnels. Cette information n'est parvenue au Commissariat que grâce à une remarquable coïncidence : la personne qui a appelé avait déjà travaillé au Commissariat. Les enquêteurs ont récupéré les documents et vérifié qu'ils provenaient de deux institutions fédérales.

Le premier groupe comportait plus d'une douzaine de dossiers de Transports Canada, dont l'un était le dossier de réclamation soumis par un employé pour ses frais de voyage (les autres n'étaient pas de nature personnelle). Ce dossier donnait force détails sur la mutation de l'employé, y compris des factures de services publics, des documents d'hypothèque et même un chèque annulé indiquant un numéro de compte bancaire.

Le second groupe de documents provenait de Santé et Bien-être social Canada et était de nature beaucoup plus délicate. Il s'agissait d'environ 370 fiches décrivant les tests de laboratoire subis par chaque personne visée (mais pas les résultats). Les enquêteurs ont immédiatement avisé les deux ministères en cause et leur ont renvoyé les documents.

Les deux ministères ont alors fait enquête et ont informé le Commissariat des résultats. Selon ces derniers, il existe des lignes directrices internes afin d'assurer que tous les documents sont retirés de tout matériel classé comme étant excédentaire. Ils ont reconnu que ces lignes directrices n'étaient pas appliquées avec toute la rigueur souhaitable et ont entrepris de sensibiliser le personnel et d'améliorer la sécurité physique. Le Commissariat n'a pas de preuves qui lui permettraient d'affirmer que des renseignements personnels sont couramment oubliés dans du matériel excédentaire, mais l'entreprise de revente a indiqué

Enquêtes spéciales

Au cours du dernier exercice, la Direction de l'observation a institué deux enquêtes spéciales sur des cas d'intractions présumées à la *Loi sur la protection des renseignements personnels*.

Vol d'ordinateur à Anciens Combattants Canada

Dans le dernier rapport annuel, il avait été question du vol d'un ordinateur portatif dans un bureau d'Anciens Combattants Canada (ACC). Cette année encore, ACC a fait savoir qu'un ordinateur renfermant des renseignements personnels avait été volé dans la maison d'un employé. L'employé était autorisé à utiliser l'ordinateur à la maison. De plus, il avait pris des précautions raisonnables pour assurer la protection de l'ordinateur et de l'information qu'il contenait. Depuis notre dernier rapport, ACC a amélioré les mesures de protection des renseignements personnels contenus dans les micro-ordinateurs. Le Commissaire n'a donc pas jugé bon d'informer les personnes concernées.

Les ordinateurs personnels se sont multipliés de façon spectaculaire au sein de la fonction publique ces dix dernières années, et pas seulement dans les bureaux. L'avènement des programmes de travail à la maison (télétravail) et d'ordinateurs portatifs aussi légers que puissants a déclenché l'essaimage des renseignements personnels. L'examen des pratiques que nous avons effectué cette année dans les ministères a révélé que les ministères étaient incapables de fournir des données exactes sur le nombre, l'emplacement et l'utilisation de leurs ordinateurs personnels.

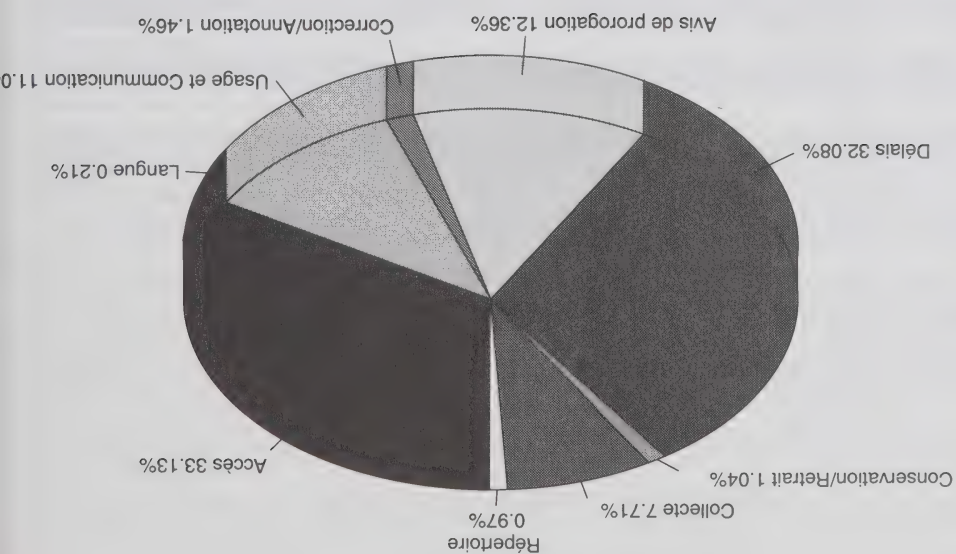
Il est curieux que ce plus récent vol à Anciens Combattants Canada ne soit que le deuxième qui ait été signalé au Commissariat. Se pourrait-il que d'autres ordinateurs se soient égarés, mais que les ministères n'aient pas prévu de mesures de contrôle suffisantes pour détecter ces pertes ou nous en aviser?

Evaluation de l'observation

L'année écoulée a été marquée par des changements et des ajustements au sein de la Direction de l'observation. En plus d'un programme de travail bien chargé (9 vérifications de conformité et 2 enquêtes spéciales, 12 vérifications de suivi, ainsi qu'une étude des technologies de l'information et de leur impact sur la vie privée), la Direction a été aux premières lignes du renouvellement opérationnel qui a touché l'ensemble du Commissariat.

Au départ, la Direction devait être une section de vérification chargée d'effectuer des examens indépendants systématiques des quelque 160 institutions fédérales régies par la *Loi sur la protection des renseignements personnels*. Mais cette tâche, allée au besoin d'examiner diverses questions découlant de la protection de la vie privée, a occasionné une charge de travail beaucoup trop lourde pour les ressources disponibles. Toutefois, le Commissariat n'entend pas renoncer à cette activité pour ne réagir qu'aux plaintes. Le pari consistait à revoir la structure et les opérations de la Direction et à contribuer au renouvellement du Commissariat.

Il en a résulté une nouvelle approche, en matière de vérification, sur les plans de la sélection (les organismes faisant l'objet d'une vérification), la portée (les éléments) et les méthodes (le processus d'enquête). Ainsi, l'attention ne sera plus axée sur les mesures de sécurité et la description des fichiers de renseignements. Les enquêteurs s'attacheront davantage à déterminer si les organismes ne recueillent que les renseignements personnels nécessaires pour leurs activités et si l'utilisation, l'échange et la communication de tels renseignements s'effectuent de façon appropriée. Ces changements devraient accroître les ressources consacrées à l'examen des questions de protection de la vie privée et, partant, nous permettre de mieux en informer le Parlement.



Plaintes réglées par motifs 1992-1993

Plaintes Régées par Institutions et Résultats

Institution	NOMBRE	Résultats		
		Bien-fondée	Résolue	Non fondée
Abandon-née				

Gendarmerie royale du Canada	60	2	53	5
Justice Canada, Ministère de la	20	5	3	12
Monnaie royale canadienne	4			4
Office national du film	2			2
Pêches et Océans	2		1	1
Revenu Canada, Douanes et Accise	53	38	3	12
Revenu Canada, Impôt	172	86	4	75
Santé et Bien-être social Canada	37	19	5	10
Secrétariat d'Etat du Canada	13	4	2	6
Service canadien du renseignement de sécurité	89		2	85
Service Correctionnel Canada	388	161	40	142
Société canadienne d'hypothèques et de logement	2			2
Société canadienne des Postes	73	30	10	30
Société du crédit agricole Canada	2		2	
Solliciteur général Canada	11		1	10
Statistique Canada	7			3
Transports Canada	30	2	5	22
Travail Canada	4	1		3
Travaux publics Canada	1			1
Voie maritime du Saint-Laurent, La	1		1	
TOTAL	1,440	441	139	757
				103

Plaintes Régées par Institutions et Résultats

Résultats			
Institution	NOMBRE	Bien-fondée	Résultats
		Bien-fondée	Résolue
		Non	Abandon- née

Affaires des anciens combattants Canada	12	2	10
Affaires extérieures Canada	14	1	3
Affaires indiennes et du Nord Canada	3		10
Agriculture Canada	11	1	9
Approvisionnement et Services Canada	1		1
Archives nationales du Canada	45	21	24
Bureau de sécurité des transports Canada	1		1
Bureau du Conseil Privé	19	2	15
Commission d'appel de l'immigration	36	2	34
Commission d'appel des pensions Canada	3	1	1
Commission de la Fonction publique du Canada	6		3
Commission des plaintes du public contre la GRC	3	1	1
Commission des relations de travail dans la fonction publique	1		1
Commission nationale des libérations conditionnelles	22	2	15
Communications, Ministère des	8		4
Conseil canadien des relations du travail	1		
Conseil du Trésor du Canada, Secrétariat	7		1
Défense nationale	112	26	77
Emploi et Immigration Canada	147	26	3
Energie, Mines et Ressources Canada	8	6	74
Environnement Canada	9	5	2

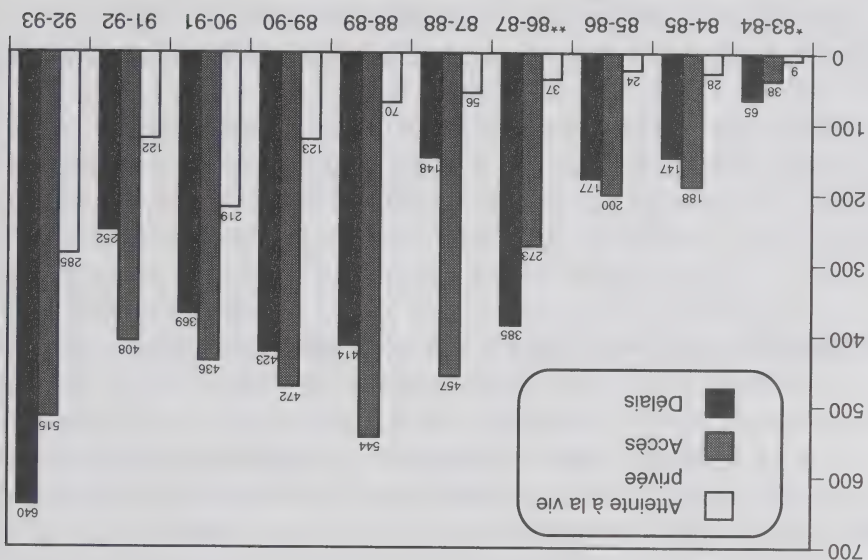
Les dix ministères les plus visés selon les plaintes reçues

Ministère		TOTAL		Accès		Délais		Autre	
Service correctionnel Canada		417		161		215		41	
Revenu Canada, Impôt		158		34		111		13	
Emploi et Immigration Canada		133		51		51		31	
Santé et Bien-être social Canada		132		90		28		14	
Société canadienne des Postes		119		54		22		43	
Service canadien du renseignement de sécurité		95		86		9		0	
Gendarmerie royale du Canada		92		62		12		18	
Revenu Canada, Douanes et Accise		92		24		60		8	
Défense nationale		72		34		22		16	
Transports Canada		48		40		4		4	
AUTRE		221		107		68		46	
TOTAL		1 579		743		602		234	

Plaintes par motifs et résultats

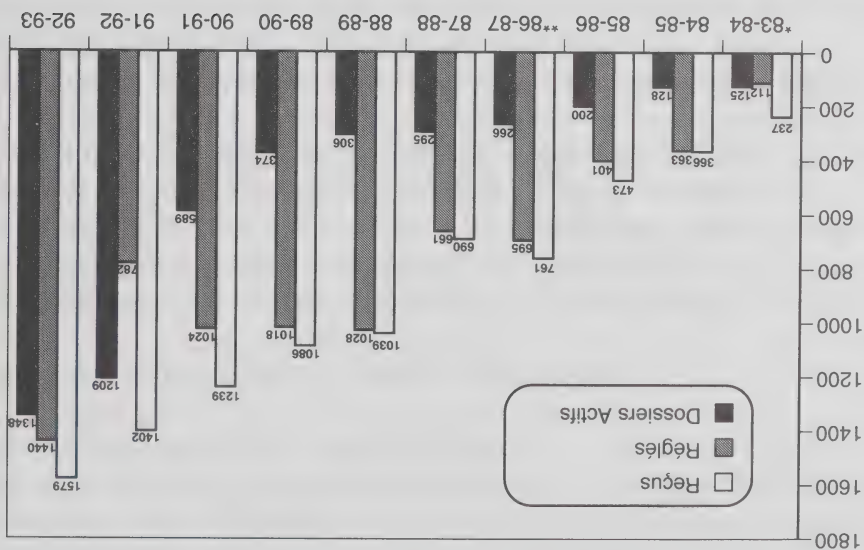
Motifs		Bien-fondée		Bien-fondée; résolue		Non fondée		Abandonnée		TOTAL	
Accès		10		114		351		40		515	
Accès	Accès	9		96		334		38		477	
	Correction/Annotation	1		4		14		2		21	
	Répertoire	0		14		0		0		14	
	Langue	0		0		3		0		3	
Attente à la vie privée		28		25		204		28		285	
Délais	Collecte	2		4		95		10		111	
	Conservation/Retrait	6		5		4		0		15	
	Usage & Communication	20		16		105		18		159	
Délais		403		0		202		35		640	
Délais		339		0		93		30		462	
Avis de prorogation		64		0		109		5		178	
TOTAL		441		139		757		103		1 440	

* 9 mois
** Nouvelle méthode de calcul



Plaintes réglées et motifs 1983-1993

* 9 mois
** Nouvelle méthode de calcul



Nombre de dossiers 1983-1993

renseignements sur les employés), le Commissaire a décidé d'accepter l'explication d'EIC, de fermer le dossier et de travailler avec le Conseil du Trésor à développer une nouvelle base de données pour conserver ces documents.

Inversion des dossiers de deux détenus

Deux détenus d'un pénitencier fédéral ont porté plainte à l'effet que les renseignements personnels de l'un avaient été communiqués à l'autre de manière non autorisée. Chacun avait demandé ses propres renseignements, mais les enveloppes, pourtant bien adressées, contenaient le mauvais dossier.

Le personnel du pénitencier a confirmé que l'inversion s'était bel et bien produite. Les dossiers avaient cependant été acheminés à l'institution dans des enveloppes scellées de sorte que l'enquête a porté sur le bureau du coordonnateur de la protection des renseignements personnels, à l'administration centrale de SCC, d'où provenaient les enveloppes.

L'enquêteur a confirmé qu'il existait des mesures visant à éviter de tels incidents. Néanmoins, le volume énorme de dossiers traités à ce bureau et le manque de personnel qualifié pour traiter ces demandes ont mené à l'inévitable. Toute procédure n'est efficace que lorsqu'elle est respectée en tout temps. Le Commissaire a conclu que les deux plaintes étaient fondées, mais il n'a fait aucune recommandation visant la mise en place de mesures supplémentaires. L'incident était probablement attribuable à une erreur humaine.

Ils se sont plaints qu'on ne leur avait pas fait connaître le but de la collecte. Ils ont aussi soutenu que les gestionnaires leur avaient ordonné de remplir ce questionnaire soi-disant facultatif, et qu'on avait exigé d'eux qu'ils consentent à toute autre utilisation et communication ultérieure de ces renseignements. Les employés ont soutenu que cela contrevenait aux dispositions sur l'utilisation et la communication de la *Loi sur la protection des renseignements personnels*. En dernier lieu, ils se sont plaints que les renseignements recueillis n'étaient pas décrits dans *Info Source* tel que l'exige la *Loi*.

Au cours de l'enquête, EIC s'est montré sensible aux préoccupations de ses employés à l'égard de la protection de leurs renseignements personnels. Le ministère avait bien essayé de respecter l'ensemble de la *Loi* dans le cadre de son projet, mais il n'en restait pas moins que certains éléments étaient discutables.

L'enquêteur n'a rien trouvé qui permettait de confirmer que les employés avaient reçu l'ordre de remplir le questionnaire. L'énoncé sur le caractère facultatif du questionnaire manquait de clarté, mais une lecture attentive permettait de saisir qu'il n'était pas obligatoire de remplir le questionnaire. Néanmoins, les représentants d'EIC ont accepté de réviser le questionnaire de sorte que la première page en indique clairement le caractère facultatif.

Les renseignements recueillis n'étaient effectivement pas décrits dans *Info Source*. Les fonctionnaires d'EIC ont expliqué que tous les éléments d'information recueillis étaient déjà décrits dans les divers fichiers usuels sur les employés, et qu'il était ainsi inutile de créer un nouveau fichier. Le Commissaire s'est objecté à cette explication, jugeant plutôt qu'il s'agissait là d'un fichier distinct de renseignements personnels recueillis dans un but précis.

Puisque plusieurs ministères ont des programmes semblables (et qu'il n'existe aucune base de données contenant de tels

La Commission nationale des libérations conditionnelles ajuste son processus

La Commission nationale des libérations conditionnelles (CNLC) doit souvent consulter d'autres organismes, tels des organismes gouvernementaux ou des forces policières provinciales, avant de rendre une décision sur une demande d'accès. Dans un de ces cas, la Commission a écrit à plusieurs organismes pour obtenir leur permission de communiquer l'information qu'ils avaient fournie au sujet du demandeur.

Tous ces organismes, sauf un, ont répondu à temps, permettant ainsi à la CNLC de traiter la demande dans le délai prévu de 60 jours. Toutefois, le procureur de la Couronne de l'Île-du-Prince-Édouard a laissé plusieurs lettres sans réponse. Après de nombreux mois, la Commission l'a finalement rejoint et il a accepté que l'information soit communiquée.

En raison du laps de temps important mis à obtenir une réponse (et de la plainte fondée du Commissaire), la CNLC a décidé de modifier son processus de consultation. Les lettres de consultation précisent maintenant que, si la CNLC n'a pas reçu de réponse d'ici à une date précise, les renseignements seront traités selon la *Loi sur la protection des renseignements personnels*. Il incombe désormais à un organisme de faire connaître rapidement son refus de communiquer l'information si tel est le cas. Les requérants n'auront donc plus à attendre inutilement pendant des mois.

Une banque de données pour les questionnaires

Plusieurs employés d'Emploi et Immigration Canada (EIC) se sont plaints par l'entremise de leur syndicat qu'un questionnaire de collecte de renseignements personnels pour le programme d'inventaire des ressources humaines du ministère portait atteinte à leurs droits en vertu de la *Loi sur la protection de la vie privée*.

Le personnel du Commissariat a recommandé que l'on avertisse les deux membres (et leurs clients dont les renseignements seraient également communiqués à titre de preuve), ce que le BCP a accepté. L'un des deux membres a alors porté plainte auprès du Commissaire.

Ce dernier a étudié les démarches du BCP, ainsi que les recommandations de la commission d'enquête, les renseignements qui avaient été divulgués et les pouvoirs du corps professionnel en matière d'assignation à produire des éléments de preuve et à mener des enquêtes.

Le Commissaire a conclu que la communication n'entreignait pas la *Loi sur la protection des renseignements personnels*. Il a aussi souligné que les pouvoirs du corps professionnel étaient suffisants pour obliger le BCP à produire les renseignements en question en vertu d'une autre disposition de la *Loi*.

Accès au consentement de «l'autre parent»

Un mari séparé a demandé au bureau des passeports des Affaires extérieures de lui fournir une copie de la déclaration, de la signature et du consentement contenus dans la demande présentée par sa femme pour l'inclusion de leurs enfants sur son passeport.

Le bureau des passeports a répondu que la demande avait été présentée par son épouse et qu'il devait obtenir son autorisation pour en obtenir une copie.

Après étude du dossier, l'enquêteur a fait part de son désaccord en soulignant que les renseignements appartenaient à l'époux puisqu'on faisait référence à «l'autre parent», et non le parent qui remplissait la demande de passeport. Le bureau des passeports n'était pas d'accord et s'est montré hésitant. Après en avoir discuté, les renseignements ont finalement été communiqués. Le Commissaire a jugé la plainte fondée et résolue.

Les documents en question avaient été soumis lors d'une commission fédérale d'enquête. Dans son rapport, la commission avait recommandé que l'organisme professionnel se penche sur la conduite de ses membres et que le BCP (dépositaire des renseignements) accède à la requête ultérieure de l'organisme et lui remette copie des renseignements. Le BCP a avisé le Commissaire en conséquence, soutenant qu'il était dans l'intérêt public, que l'organisme professionnel maintienne le niveau de ses normes.

Le cas illustre bien les limites touchant les pouvoirs du Commissaire et les droits des personnes affectées par ces communications d'«intérêt public». Il permet également de comprendre pourquoi il revient au personnel d'étudier les avis de communication : le Commissaire ne doit pas juger d'avance la communication et être ainsi empêché de pouvoir statuer sur toute plainte subséquente.

L'année dernière, le Commissariat signalait avoir reçu une plainte déposée à l'endroit du Bureau du Conseil privé (BCP) suite à la communication de renseignements personnels sur deux de ses membres à leur organisme professionnel.

Une communication faite dans l'intérêt public suscite une plainte

La plainte a été jugée fondée.

L'enquête a confirmé que chaque établissement pénitentiaire conservait un registre informatisé ou manuel de tous les griefs soumis par les détenus. Tous ces établissements peuvent facilement identifier et localiser les dossiers de grief d'un détenu d'après le nom de ce dernier. L'information additionnelle de localisation n'était donc pas nécessaire. SCC a reconnu qu'il était en mesure de retrouver un dossier en fonction d'un nom et a accepté de modifier ses exigences ayant trait à l'accès à ces renseignements.

relatifs à la santé et à la sécurité au travail, on devait veiller à ce que les employés qui reviennent d'un congé de maladie ne mettent pas en danger leurs collègues ou eux-mêmes. L'Administration a aussi soutenu que la collecte de renseignements médicaux aidait les employés à demeurer honnêtes et jouait un rôle important dans le contrôle de l'absentéisme et la réduction des coûts.

Le Commissaire à la protection de la vie privée admet que les employeurs ont le droit de s'assurer que l'absence d'un employé est justifiée et qu'il peut exister des situations où il est nécessaire de recueillir des renseignements médicaux auprès des employés avant d'approuver leurs demandes de congés de maladie. Toutefois selon le Commissaire, la collecte et l'évaluation des renseignements médicaux ne devraient pas être effectuées par du personnel non qualifié. Le Commissaire a estimé que la plainte était fondée puisque seul un médecin compétent devrait avoir le droit de recueillir des renseignements médicaux en vue d'évaluer la condition d'un employé.

Les représentants de l'Administration de la voie maritime du Saint-Laurent ont réagi en modifiant leurs procédures de collecte de renseignements relativement aux congés médicaux, en place depuis les années 1960. Désormais la nature de la maladie n'a plus à être révélée aux surveillants. Lorsque cela est nécessaire, ces renseignements seront recueillis et revus seulement par un médecin.

Repères supplémentaires inutiles

Un détenu d'un des pénitenciers de Service Correctionnel Canada a demandé accès à ses dossiers de grief. Il s'est par la suite plaint au Commissaire lorsque SCC a refusé de traiter sa demande en alléguant qu'il n'avait pas fourni tous les renseignements nécessaires à la localisation des dossiers.

deux ans pour les documents sur papier et de 25 ans pour les documents sur autres supports.

L'enquêteur devait avant tout déterminer la vraie période de conservation que le ministère appliquait aux deux fichiers. Les représentants d'EIC ont expliqué que les renseignements étaient en effet conservés pendant deux ans par les centres d'emploi du Canada, puis transférés aux archives du ministère où ils étaient conservés pendant cinq autres années avant d'être détruits. Seules les statistiques et les évaluations de programmes (non les renseignements personnels) sont transférés sur bande magnétique et conservés pendant 25 ans.

Le Commissaire a conclu que les renseignements n'avaient pas incorrectement été détruits et que la plainte n'était pas fondée. Néanmoins, il s'est dit préoccupé par la confusion, les nombreux renvois de la requête du plaignant et les explications contradictoires sur la non-existence des renseignements. Il a demandé à EIC de clarifier sa description des périodes de conservation publiées dans *Info Source*—un outil dont dépend la population pour avoir accès à ses dossiers.

Collecte non autorisée de renseignements médicaux

Un employé de l'Administration de la voie maritime du Saint-Laurent a porté plainte auprès du Commissaire lorsqu'on a refusé de lui payer deux jours de congé de maladie parce qu'il refusait de révéler à son surveillant la nature de sa maladie. L'enquête a révélé que la politique de l'Administration exigeait que ses employés se portant malades fournissent des détails médicaux sur le formulaire de demande de congé. Le surveillant immédiat de l'employé étudiait alors ces renseignements et déterminait si l'état justifiait le paiement du congé.

L'Administration a soutenu que les surveillants devaient recueillir et évaluer ces renseignements parce que, selon les règlements

d'identification au sujet des détenus qui sont séropositifs ou atteints du SIDA.

Le Commissaire a jugé raisonnable que la GRC donne aux gardiens des renseignements sur les individus qui posent un risque pour les employés et les autres prisonniers. Il a conclu que l'affichage n'avait pas violé la Loi. Le Commissaire demeure néanmoins préoccupé de ce que certains organismes dressent des répertoires des personnes séropositives et il sait gré aux deux organismes de soutien aux sidéens de la rapidité de leur intervention et à la GRC de sa réaction immédiate.

La vaise de la bureaucratie

Un homme à la recherche de renseignements au sujet de sa participation à des programmes de formation d'Emploi et Immigration Canada en 1975 a déposé auprès du Commissaire une plainte à l'effet qu'on l'avait fait tourner en rond. Il s'était tout d'abord rendu à son Centre d'emploi local pour se faire dire que le ministère ne conservait pas de renseignements remontant à 1975. Une consultation d'*Info Source* (le répertoire des fonds d'information du gouvernement) lui a confirmé que les dossiers de formation étaient pourtant conservés pendant 25 ans. Rassuré, il s'est rendu au bureau régional de Toronto et a fait une nouvelle tentative.

Le bureau régional l'a renvoyé à son Centre d'emploi local qui lui a répété que l'information n'existait pas. Cette fois, sa demande a été renvoyée aux Archives nationales. Au cours de ces tergiversations, le plaignant a reçu plusieurs explications contradictoires. Ainsi, on lui a dit que les renseignements n'étaient conservés que pendant deux ans, puis sept ans. *Info Source* décrit la période de conservation d'un des fichiers comme étant perpétuelle mais, pour un second fichier, de

Le Commissaire a fait enquête pour déterminer si la GRC aurait dû recueillir des renseignements sur la séroposivité de ces cinq personnes, évaluer comment l'organisme utilisait ces renseignements et si leur communication était justifiée.

L'enquête a permis d'établir que les photographies et les renseignements provenaient des dossiers opérationnels du détachement. Les dossiers identifiaient les cinq personnes comme des récidivistes connus enclins à la violence, représentant une menace pour la sécurité des agents de police et des gardiens. Toutes les cinq s'étaient volontairement reconnues porteuses du virus VIH.

Ces personnes étaient bien connues des gardiens à temps plein affectés au détachement, mais le personnel a suggéré d'afficher les renseignements dans la salle des gardes où dix gardiens occasionnels (qui remplace le personnel régulier en vacances ou en congé de maladie) pourraient en prendre connaissance.

L'enquêteur a découvert que les prisonniers et le public n'avaient pas accès à la salle des gardes. En fait, même les agents de police n'y ont habituellement pas accès. Cependant, la salle est très souvent laissée sans surveillance lorsque les gardiens sont occupés ailleurs dans le bloc cellulaire.

Il était évident qu'en raison de leur petite taille, les photographies et les documents n'étaient pas reconnaissables du comptoir situé à l'avant du bureau, ni même de l'embrasure de la porte. Le tableau d'affichage étant situé sur le même mur que la porte et le comptoir, il fallait obligatoirement passer derrière le comptoir pour s'approcher du tableau et lire les affiches. L'enquêteur n'a pu déterminer qui avait vu les documents.

Depuis, les renseignements ont été enlevés du tableau d'affichage et rangés dans un tiroir d'un des bureaux. La GRC prépare actuellement une politique visant à contrôler les renseignements

Lors de son inscription pour un emploi d'été, le plaignant avait refusé de fournir son NAS et avait demandé pourquoi EIC avait besoin de cette information. Il a soutenu que la question avait été soumise à un gestionnaire qui a alors extrait le NAS du plaignant des dossiers ministériels avant de lui parler.

EIC a déclaré qu'il était raisonnable qu'un gestionnaire utilise le NAS afin d'extraire le dossier du client avant de le rappeler et soit ainsi mieux préparé à lui répondre. Le Commissaire a accepté l'explication et a déclaré que la plainte n'était pas fondée.

Toutefois, le ministère a dû expliquer pourquoi un client devait fournir son NAS lorsqu'il s'inscrit pour un emploi. Selon EIC, cela visait simplement à offrir le plus vaste éventail possible des services disponibles aux clients du ministère. Le NAS est la seule façon pratique d'identifier des clients dotés d'habiletés particulières afin de les orienter vers des emplois appropriés.

Néanmoins, EIC a convenu de ne plus demander le NAS à un client lorsque ce dernier s'y oppose. Toutefois, le client sera averti que le fait de ne pas communiquer son NAS limitera les services qu'EIC est en mesure d'offrir et pourrait signifier la perte de certaines références au niveau du service de présentation d'emplois. Ce sera au client de décider de fournir ou non son NAS.

Affichage irréfléchi identifiant des porteurs du VIH

Le Commissaire à la protection de la vie privée a reçu une plainte du Réseau sidéen de la Colombie-Britannique à l'effet que la GRC avait affiché, sur un babillard d'un détachement local, les photographies et les descriptions de cinq personnes porteuses du VIH. Après que quelqu'un ait vu l'affichage et en ait informé l'une de ces personnes, cette dernière a porté plainte auprès d'un groupe local de soutien aux sidéens.

Une plainte d'un homme à l'effet qu'Emploi et Immigration Canada (NAS) a mené EIC à modifier la façon dont le ministère inscrit les clients à la recherche d'un emploi.

Le NAS—facultatif pour la recherche d'un emploi

Selon le Commissaire, le ministère des Affaires extérieures a agi de façon appropriée en rejetant la demande du plaignant et il a jugé que la plainte n'était pas fondée.

Le Commissaire a jugé que les renseignements du passeport constituaient des renseignements personnels au sujet du fils. La Loi n'autorise la communication des renseignements personnels seulement qu'à la personne concernée sauf si cette dernière consent à leur communication à un tiers (il existe des exceptions particulières). Puisque l'enfant est mineur, le *Règlement sur la protection des renseignements personnels* exige le consentement du tuteur légal de la personne—dans le cas présent, l'ancienne femme du plaignant.

Un homme s'est plaint au Commissaire que le ministère des Affaires extérieures lui avait refusé accès aux dossiers de passeport de son fils. Le père estimait qu'il était en droit de consulter ces dossiers parce que son fils était mineur.

Consentement du tuteur légal exigé pour un mineur

Le Commissaire a conclu que la *Loi sur la protection de la vie privée* ne justifiait une telle communication. La Loi autorise la communication de renseignements personnels en réponse à un mandat ou à une ordonnance de la cour, mais l'organisme n'avait obtenu aucun des deux. Le Commissaire a conclu que la communication n'était pas justifiée et il a jugé la plainte fondée.

entreprind des centaines de mesures de dotation chaque année : il est quasi inévitable qu'on lui fournisse à l'occasion des renseignements médicaux non sollicités durant des vérifications de référence. Néanmoins, le Commissaire estime que le ministère doit veiller à ne pas recueillir plus de détails personnels qu'il n'en a besoin dans le simple but d'évaluer l'assiduité et la ponctualité d'un candidat.

Le Commissaire a conclu que les renseignements médicaux n'étaient pas nécessaires à la dotation et que la plainte était fondée. Toutefois, il a rejeté une deuxième plainte à l'effet qu'EIC avait fait un mauvais usage des renseignements lorsqu'il est apparu que c'était en raison de son dossier d'assiduité (qui était pertinent) que la personne avait été disqualifiée.

EIC a retiré des dossiers de la personne toutes les mentions faites par le surveillant sur la maladie de cette dernière. En outre, le ministère a accepté de publier des lignes directrices rappelant aux gestionnaires la démarche appropriée à adopter pour mener une vérification des références en respectant la Loi sur la protection des renseignements personnels et la Loi sur les droits de la personne. Le Commissaire a jugé que la question était résolue.

Ordonnance de la cour exigée pour une communication

Une employée de Service correctionnel Canada (SCC) a déposé une plainte auprès du Commissaire à l'effet que son directeur avait communiqué à un tiers une copie d'un rapport d'enquête de sécurité contenant des renseignements personnels la concernant. Le directeur a confirmé avoir remis une copie du rapport au directeur d'un organisme d'assistance postpénale ayant passé contrat avec SCC, et ce à la demande de l'organisme, contre lequel la plaignante avait intenté une poursuite.

Le Commissaire a convenu qu'un employeur a le droit de signaler à un représentant du syndicat qu'un membre est impliqué dans une grève illégale, mais qu'il n'avait pas le droit de remettre une copie de la lettre de réprimande précisant quelle mesure disciplinaire serait prise. Le Commissaire a jugé que la plainte était fondée.

Pas de communication de renseignements médicaux détaillés au cours d'une vérification des références

Une employée d'EIC a porté plainte auprès du Commissaire à l'effet que le ministère avait recueilli de façon non autorisée des renseignements médicaux confidentiels et inexacts à son sujet en faisant une vérification des références auprès d'un surveillant, puis qu'il avait utilisé ces renseignements pour l'éliminer de la liste des candidats qualifiés.

L'enquête a confirmé que, lors d'un concours dans l'un de ses centres d'emploi, le personnel d'EIC avait communiqué par téléphone avec le dernier surveillant des candidats qualifiés. Le surveillant a été interrogé sur l'assiduité et la ponctualité de la candidate au cours de la dernière année, et il a fourni des détails médicaux précis qui ont alors été portés au dossier.

La collecte de renseignements au sujet de maladies ou de blessures dans le cadre d'une vérification des références pose toujours de sérieux problèmes dans le contexte de la *Loi sur la protection des renseignements personnels*. Le fait de fournir sans motif valable des détails sur la santé ou la vie des gens peut nuire à ces derniers. Le Commissaire était préoccupé par l'exactitude des renseignements médicaux recueillis au cours de ce processus, ainsi que par la validité des conclusions que le personnel pourrait tirer en se basant sur ces renseignements.

La *Loi sur la protection des renseignements personnels* interdit à un ministère de recueillir des renseignements personnels qui n'ont pas de « lien direct avec ses programmes ou activités ». EIC

elles auraient dû être conservées et mises à la disposition du plaignant. Puisqu'elles n'avaient pas été conservées, le Commissaire a jugé que la plainte était fondée.

À la suite de l'enquête, le ministre de la Justice a confirmé au Commissaire que les comités de sélection devront désormais conserver les notes que leurs membres prennent et utilisent dans leur prise de décision. Les notes manuscrites seront confiées au représentant du personnel et feront partie du rapport final du comité (à moins qu'elles n'y soient incorporées textuellement). Le Commissaire a accepté les observations du ministre à l'effet que les ramifications de ce cas étaient suffisamment importantes pour compenser le délai.

Un avis de discipline ne concerne pas le syndicat

Un employé d'Emploi et Immigration Canada (EIC) a déposé une plainte auprès du Commissaire parce que son surveillant avait, au cours de la grève de l'Alliance de la fonction publique du Canada (AFPC) en octobre 1991, communiqué de façon non autorisée à un autre employé des renseignements sur des mesures disciplinaires prises à son égard.

L'enquête a révélé que le plaignant était un « employé désigné », ce qui signifie qu'il devait travailler pendant la grève. Toutefois, un matin, il ne s'est pas présenté au travail et il a été aperçu plus tard sur la ligne de piquetage. Son surveillant lui a écrit une lettre pour le réprimander de son absence sans autorisation et il a tenté sans succès de la lui remettre.

Après avoir averti l'employé de retourner immédiatement au travail (et lui avoir signalé les conséquences financières d'un refus), le gestionnaire a déposé la lettre sur la table de travail du plaignant. Il en a également remis une copie au coordonnateur de la grève de l'AFPC, qui était aussi le délégué syndical du plaignant.

Accès aux notes prises lors d'un concours

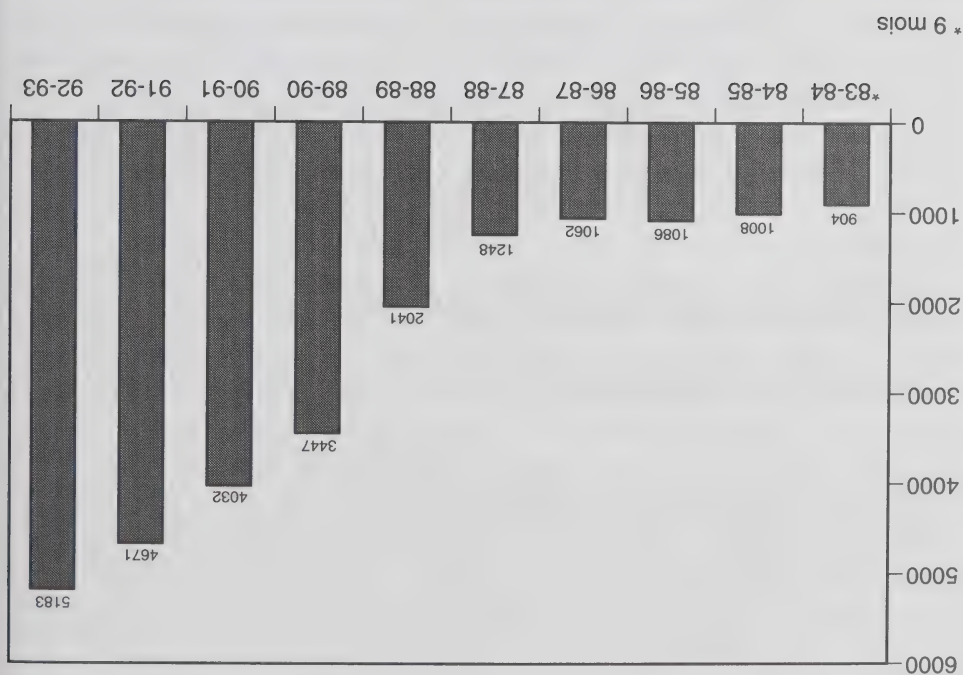
Une plainte déposée à l'endroit du ministère de la Justice a créé un précédent important pour l'accès aux notes manuscrites prises par les membres du comité de sélection lors des concours.

Un homme a demandé au ministère de la Justice des copies de tous les documents rassemblés au cours de son entrevue. Il a porté plainte auprès du Commissaire lorsque le ministère n'a pu retrouver les notes des intervieweurs.

L'enquêteur a découvert que tous les membres du comité de sélection avaient pris des notes pour faciliter l'évaluation des candidats au cours des entrevues. Les notes prises par les trois membres du comité avaient été détruites une fois le poste doté. Le quatrième membre (une agente de dotation) se rappelle avoir joint ses notes aux documents transmis au personnel lorsqu'elle a quitté le ministère peu après les entrevues. Cependant, une recherche menée dans les dossiers de dotation du ministère n'a rien permis de retrouver. Le ministère a supposé que les notes avaient accidentellement été détruites ou perdues.

Le Commissaire était disposé à admettre que tous les employés prennent à l'occasion des notes personnelles qui ne peuvent pas être jugées comme «relévant du contrôle» de leur ministère mais, il n'était pas convaincu que cela était ici le cas. À son avis, les notes des membres du comité de sélection servent à choisir un candidat—but administratif—et devraient donc faire partie du dossier de dotation. Cela signifie que l'on peut y avoir accès en vertu de la *Loi sur la protection des renseignements personnels*.

Après des consultations poussées, le ministère de la Justice s'est finalement rallié à la thèse du Commissaire. Le ministère n'a pu déterminer le contenu exact des notes prises au sujet du plaignant. Toutefois, il a admis que, puisque le comité de sélection avait pris en considération les notes pour rendre sa décision, celles-ci avaient donc été utilisées à des fins administratives et



Requêtes 1983-93

fins d'identification. Il n'existe pas de loi pertinente. La prise de photos est-elle une nouvelle mode?

Les demandes de renseignements au sujet du NAS se poursuivent—nous en avons reçu 549 cette année. Le Commissariat conseille à ceux et à celles qui ne désirent pas communiquer leur NAS aux entreprises privées, aux propriétaires et aux organismes non assujettis à une loi régissant le NAS, de poser les questions suivantes :

- Avez-vous besoin de mon NAS afin de respecter une loi ou un règlement?
- Sinon, pourquoi en avez-vous besoin et quelle utilisation en ferez-vous?
- Le tiendrez-vous confidentiel?
- Si je refuse de vous le donner, quelles seront les conséquences?
- Accepteriez-vous une autre pièce d'identité?

peut qu'orienter les personnes vers les institutions financières en question—lesquelles ont chacune leur propre politique de gestion et d'utilisation des renseignements personnels.

Les agents de requêtes doivent souvent expliquer que la Loi ne traite que d'un aspect de la vie privée. Ainsi, un homme revenant au pays après une affectation à l'étranger s'est plaint auprès du Commissaire de la grossièreté des douaniers et de la fouille de ses dossiers et ses effets personnels. Il voulait savoir quels étaient ses droits en vertu de la Loi sur la protection des renseignements personnels. On lui a expliqué que la Loi sur les douanes autorisait les douaniers à examiner les biens et le courrier et que leurs activités et leur impolitesse n'étaient pas assujetties à la Loi sur la protection des renseignements personnels.

Il arrive que des cas qui pourraient constituer des plaintes officielles sont traités de manière officielle à la demande de l'interlocuteur, tel le cas d'un employé travaillant pour une entreprise qui participe au programme de partage de l'emploi avec Emploi et Immigration Canada (EIC). L'employé était inquiet de ce que le ministère lui avait fait parvenir des documents par l'entremise de son employeur.

La compagnie devait vérifier les relevés des prestations de son personnel afin d'apporter les redressements salariaux nécessaires, mais l'employé ne jugeait pas que la compagnie avait le droit de connaître son code d'accès téléphonique. Ce code permet aux prestataires d'assurance-chômage de se renseigner par téléphone sur leurs prestations. EIC s'est penché sur le problème et a accepté de retirer les codes des documents. Il a également averti les employés de changer leur code.

Trois personnes ont communiqué avec le Commissariat afin de savoir si Moneymart, un magasin de vidéos et un de gros appareils ménagers, avaient le droit de les photographier à des

Le nombre de demandes de renseignements a augmenté de 10 p. 100 cette année pour atteindre 5 183, dont 4 865 appels téléphoniques, 274 lettres et 44 visites.

Près de 55 p. 100 des demandes concernaient les droits de la personne en vertu de la Loi; toutefois, 20 p. 100 avaient trait à des questions de protection de la vie privée qui ne relevaient pas de la compétence du Commissaire à la vie privée, mais de celle d'autres organismes du secteur public ou d'entreprises privées. Le reste des demandes relevaient soit d'un autre organisme ou d'un sujet autre que la protection de la vie privée. Dans de tels cas, les agents de requêtes redirigent les demandeurs vers l'organisme ou le ministère approprié.

Plusieurs personnes se sont dites préoccupées par le fait que les employés des Postes leur demandaient leurs numéros de carte d'identité lors de la réception de colis ou de courrier recommandé. Le Commissariat a examiné la procédure de la Société canadienne des Postes, laquelle exige qu'une personne venant chercher un colis ou du courrier recommandé produise des papiers d'identité acceptables et que l'employé des Postes note ces détails dans un registre.

Le Commissaire a reconnu que la SCP devait respecter une telle procédure afin de s'assurer que la personne réclamant le colis est bien le bénéficiaire. L'information est consignée afin de retracer la piste lorsque des biens de valeur ou des documents se perdent. Le personnel du Commissariat a également confirmé que les registres étaient conservés dans un endroit interdit au public.

Les agents de requêtes continuent de recevoir nombre d'appels reliés à la collecte, à l'utilisation et à la communication de renseignements personnels par des institutions financières. Puisque les banques ne sont pas assujetties à la Loi sur la protection des renseignements personnels, et que le Bureau du surintendant des institutions financières ne dispose d'aucun mécanisme de traitement de telles plaintes, notre personnel ne

Deuxièmement, le Commissaire se demandait comment ASC pourrait protéger les actionnaires contre l'utilisation ou la vente subéquente des listes. Une fois que des renseignements sont communiqués, le gouvernement n'a aucun recours juridique pour en empêcher la reproduction, la vente ou toute autre utilisation.

Enfin, le Commissaire s'interrogeait sur la façon dont le comptable s'y prendrait pour retracer les actionnaires à l'aide des mêmes adresses que détenait ASC. S'il existait un moyen, il a encouragé ASC à s'en servir et ainsi à faire économiser les frais demandés aux actionnaires. Les deux Commissaires ont convenu qu'ASC devait faire preuve d'une plus grande détermination dans ses efforts pour rejoindre les actionnaires, mais le Commissaire à la protection de la vie privée n'était pas convaincu que la divulgation des renseignements à un tiers était la mesure qui s'imposait.

Le comptable n'a pas reçu les listes qu'il avait demandées, mais sa plainte a incité le ministère à écrire de nouveau à tous les actionnaires et à examiner d'autres moyens pour rejoindre ceux qui n'auront pas répondu.

ASC détient ces listes parce que la société a été dissoute en 1983 et que la valeur des actions non réclamées, soit 120,14 \$ chacune, a été versée au Trésor public. Les actionnaires inscrits peuvent présenter une demande de remboursement à ASC.

Il semblerait qu'ASC avait écrit à chacun des actionnaires lors de la liquidation de la société afin de leur expliquer les modalités d'encassement des actions. Ce ministère a aussi passé des annonces dans de grands journaux canadiens et étrangers. Environ 80 p. 100 des actions ont été remboursées et le ministère continue de recevoir des demandes de personnes figurant sur les listes. En raison de la plainte du comptable, le ministère a envoyé un autre rappel aux actionnaires. Il a soutenu que tout actionnaire qui ne sait pas exactement comment obtenir le remboursement n'a qu'à communiquer avec Petro-Canada ou tout courtier en valeurs mobilières.

Il est d'intérêt public de s'assurer que le gouvernement fait des efforts raisonnables pour retracer ceux pour qui il détiendrait l'argent. Dans ce cas, toutefois, le Commissaire avait des réserves. Il se demandait notamment s'il était dans le meilleur intérêt du public que des renseignements soient communiqués, sans le consentement des actionnaires, à un tiers qui comptait leur rendre un service moyennant 15 à 40 p. 100 de la valeur nominale des actions. La divulgation de ces renseignements semblait beaucoup plus dans l'intérêt du comptable que dans celui des actionnaires.

Le fait de divulguer ces renseignements ne garantissait pas non plus que les intérêts de tous les actionnaires seraient servis. Le Commissaire doutait que le comptable juge intéressant de retracer les actionnaires qui ne détiennent que trois actions ou moins et qui forment au moins la moitié de la liste. En outre, 60 p. 100 des personnes qui sont inscrites sur cette dernière habitent à l'étranger.

fonctionnaires—la CFP a conclu qu'il y allait de l'intérêt public de fournir tous les détails du processus. Le rapport renfermait les noms de tous les candidats qualifiés qui étaient apparentés à des employés des douanes, les titres (mais non les noms) des employés en question, ainsi qu'un court résumé général de l'expérience de travail de divers candidats.

Malheureusement, le Commissaire n'a été informé que le lendemain de la diffusion du rapport au *Winnipeg Free Press*, et n'a donc pas eu la possibilité de prévenir les personnes concernées de la publicité dont elles feraient probablement l'objet. La CFP a reconnu son erreur, mais elle a indiqué qu'elle se sentait pressée d'agir devant les demandes d'explications répétées de la part des médias. Le Commissaire a décidé de communiquer par écrit avec toutes les personnes concernées afin de leur expliquer le processus de même que leurs droits en vertu de la Loi sur la protection des renseignements personnels.

Les noms des actionnaires de Petro-Canada ne sont pas divulgués

Approvisionnement et Services Canada (ASC) a fait savoir au Commissaire à la protection de la vie privée que le Commissaire à l'information lui avait recommandé de communiquer les noms et les dernières adresses connues des actionnaires des Entreprises Petro-Canada Inc. à un «comptable enquêteur».

Le ministère avait rejeté la demande d'accès à l'information du comptable parce que les renseignements étaient de nature personnelle et qu'ils étaient donc protégés. Le comptable a déposé une plainte auprès du Commissaire à l'information en faisant valoir qu'il serait à l'avantage des actionnaires qu'il puisse utiliser les listes d'ASC pour les retracer et obtenir—moyennant rétribution—le remboursement des sommes auxquelles les actionnaires avaient droit.

Compte tenu de la gravité des accusations—et du mandat de la CFP de respecter le principe du mérite dans l'embauchage des

une du syndicat des employés des douanes.
aux accusations et d'autres plaintes ont suivi, 25 au total, dont des surintendants des Douanes. Les médias locaux ont fait écho qu'au moins trois des individus embauchés étaient apparentés à Plusieurs candidats qui n'avaient pas été retenus se sont plaints

reçu une offre d'emploi.
qualifiées ont été classées selon leur mérite et 11 d'entre eux ont candidats qui avaient réussi l'épreuve écrite. Les 20 candidats présélection, des fonctionnaires des douanes ont interviewé 279 pourvoir à Revenu Canada (Douanes et Accise). Suite à la La CFP avait reçu plus de mille candidatures pour les postes à

qu'elle avait l'intention de publier son rapport.
Commissaire qu'elle avait fait enquête sur ces accusations et de l'embauchage de tous les fonctionnaires fédéraux, a avisé le *Press*. La Commission de la fonction publique (CFP), responsable des accusations de favoritisme sont parues dans le *Winnipeg Free* d'inspecteurs des douanes à Winnipeg et à Emerson (Manitoba), À la suite d'un concours visant à pourvoir des postes

Des accusations de favoritisme donnent lieu à la divulgation de renseignements personnels

avec les élections.
satisfait du moment que les listes ne sont utilisées qu'en rapport rejoindre les électeurs en période électorale. Le Commissaire est demandeurs politiques, dans l'intérêt des candidats qui veulent l'obtention de ces listes, mais il ne les communique qu'aux Elections Canada reçoit de nombreuses demandes pour

dans le cadre du référendum constitutionnel.
utiles parce qu'elles reflètent le récent dénombrement effectué sollicitation de dons. Les listes actuelles sont particulièrement

Canada en vue d'obtenir des renseignements figurant dans le passeport d'un membre de l'équipe.

L'équipe n'avait pas réussi à se classer parmi les douze premières aux compétitions préliminaires et ses membres s'étaient dispersées. Toutefois, deux pays classés n'ayant pu réunir une équipe complète, les Canadiennes ont été invitées à participer. Les organisateurs ont alors tout mis en œuvre pour regrouper l'équipe et fournir immédiatement les données figurant dans les passeports aux organisateurs des Jeux aux fins de sécurité et d'identification. Incapables de rejoindre l'une des membres, les organisateurs se sont adressés aux Affaires extérieures pour obtenir le numéro et la date d'expiration de son passeport.

Le ministère a conclu qu'il était dans l'intérêt public que l'équipe en entier soit réunie et que cela représentait également un avantage pour le membre visé. Le ministère a informé le Commissaire qu'il allait communiquer l'information et les organisateurs ont rejoint le membre manquant 12 heures plus tard.

Listes électorales et partis politiques

Une vérification de conformité menée en 1992 auprès d'Elections Canada a révélé que les listes électorales étaient communiquées de façon courante aux partis politiques et aux candidats pour des « raisons d'intérêt public » sans que le Commissaire en soit avisé. Par suite de l'examen, le Commissaire a reçu son premier avis de communication en janvier 1993.

Les listes sont dressées à partir du dénombrement effectué de porte à porte durant la campagne électorale. Des données tels le nom de famille, le prénom, le sexe et l'adresse y figurent pour chaque électeur admissible dans la circonscription, et les listes sont disponibles sur papier ou support électronique. Les partis politiques et les candidats s'en servent pour des envois promotionnels, la sollicitation porte à porte des suffrages et la

L'équipe féminine d'escrime du Canada a eu une occasion de dernière minute de participer aux Jeux de Barcelone, ce qui a suscité un appel urgent au ministère des Affaires extérieures du

Divulguation des détails d'un passeport aux organisateurs des Jeux olympiques

renseignements personnels.
ses droits propres en vertu de la Loi sur la protection des qu'elle comprenait les obligations du gouvernement de même que l'association. Le Commissaire a écrit à l'infirmière afin de s'assurer professionnels se conformer à leur code de conduite et a avisé déterminé qu'il était dans l'intérêt public d'assurer que les syndicat avait conseillé à l'infirmière de ne pas le faire. Le SCC a à leur association de tout écart au code de déontologie mais le l'association de l'incident. Les infirmières sont tenues de faire part Le comité d'enquête du SCC a recommandé d'informer

prélever le sang d'un autre détenu.
fédéral. Une autre infirmière avait ensuite utilisé la seringue pour contaminée par le VIH sur un comptoir dans un pénitencier Columbia le nom d'une infirmière qui avait laissé une seringue qu'il fournirait à la Registered Nurses Association of British Dans un autre cas lié au VIH, le SCC a informé le Commissaire

Le nom d'une infirmière est dévoilé à son association professionnelle

informé l'homme de la divulgation.
ce fait aux parents. Le SCC a accepté et le Commissaire a la détection du VIH. Le Commissaire a enjoint le SCC de signaler puisqu'il peut se passer des années entre l'exposition d'un sujet et nécessairement que la santé des enfants n'était plus menacée, séro-négativité de l'agresseur présumé ne signifiait pas familles. Toutefois, le Commissaire a fait valoir au SCC que la Comme les résultats étaient négatifs, le SCC voulait rassurer les

Communications au Commissaire

La Loi sur la protection des renseignements personnels a pour objectif général d'empêcher les organismes fédéraux de divulguer des renseignements personnels sur une personne sans le consentement de celle-ci, mais il y a des exceptions. Deux de ces exceptions obligent l'organisme à aviser par écrit le Commissaire à la protection de la vie privée : une communication pour des «raisons d'intérêt public» ou lorsque la personne concernée en tirerait un avantage. Il y a eu 48 avis de ce genre cette année.

La Loi confie au responsable de l'organisme, et non pas au Commissaire, le soin de déterminer ce qui constitue une «raison d'intérêt public». Le rôle du Commissaire consiste à examiner la proposition et à informer les personnes concernées s'il le juge à propos. Le Commissaire n'a pas le pouvoir d'interdire une communication, mais il peut entreprendre une enquête s'il est fortement en désaccord. La personne concernée n'a pas de moyen, non plus, pour bloquer la communication; elle a le droit, toutefois, de déposer une plainte auprès du Commissaire, mais seulement une fois la communication faite.

Le personnel du Commissariat examine les avis des organismes, ce qui permet ainsi au Commissaire d'être libre de considérer toute plainte ultérieure.

Il n'est pas toujours facile pour les responsables des institutions fédérales d'évaluer l'intérêt public, comme l'illustrent certains des avis reçus durant l'année.

Communication de profil sérologique (VIH)

Le Service correctionnel du Canada (SCC) a avisé le Commissaire qu'il allait divulguer si un homme soupçonné d'avoir agressé sexuellement deux jeunes filles était séropositif ou non. L'homme, en libération conditionnelle à ce moment-là, avait refusé aux pères des jeunes filles l'accès aux résultats des tests sanguins qu'il avait subis volontairement lors de son arrestation.

Origine des plaintes réglées

	TOTAL
Terre-Neuve	8
Ile-du-Prince-Édouard	3
Nouvelle-Écosse	27
Nouveau-Brunswick	30
Québec	153
Région de la Capitale nationale—Québec	13
Région de la Capitale nationale—Ontario	156
Ontario	588
Manitoba	63
Saskatchewan	55
Alberta	101
Colombie-Britannique	216
Territoires du Nord-Ouest	2
Yukon	19
Hors Canada	6
	1 440

documents se rapportant à leurs griefs alors que les gestionnaires de la SCP n'ont aucun droit équivalent d'accès aux dossiers du syndicat.

Cette opinion selon laquelle la Loi sert les intérêts des employés impliqués dans des conflits de travail a compliqué la résolution de certaines plaintes. Le fait que le Commissariat ait, pour la première fois de son existence, porté un cas devant la cour (le refus de la SCP de divulguer le nom d'un témoin lors d'une enquête interne au sujet d'un grief) illustre bien le problème.

Autres ministères

Plus d'une centaine des 172 enquêtes effectuées à la suite de plaintes déposées contre Revenu Canada—Impôt l'ont été pour le compte d'un seul individu et portaient sur des délais. Les responsables des Douanes ont également éprouvé des difficultés à respecter la période prescrite de 30 jours : 36 des 44 plaintes déposées ont été jugées fondées.

Des félicitations sont de mise pour les efforts que la GRC a déployés pour respecter les dispositions de la Loi relatives à l'accès. Aucune des 47 enquêtes sur des plaintes concernant un délai ou un refus d'accès ou de correction n'a donné raison aux plaignants. Le Service canadien du renseignement de sécurité respecte aussi les délais et les dispositions de la Loi. Seulement 2 des 89 plaintes à son endroit étaient fondées et toutes deux ont été résolues.

Malgré tout, il est décourageant d'avoir à signaler qu'après dix ans d'application de la Loi, nombre de ministères éprouvent encore de la difficulté à répondre aux demandes de façon appropriée et en temps opportun.

Le ministère a aussi fait l'objet de plusieurs plaintes quant aux délais de traitement des demandes—dans 18 cas sur 37, on a donné raison aux plaignants.

Société canadienne des Postes (SCP)

Le nombre des nouvelles plaintes sur les délais (54) et l'accès (22) déposées à l'endroit de la SCP est le même que l'an dernier. Cependant, la SCP continue d'être la cible de nombreuses plaintes liées à la collecte, l'utilisation, la communication et la conservation des dossiers sur les employés. Les 43 plaintes de ce type représentent 36 p. 100 des 119 plaintes déposées au total contre la SCP, qui détient ainsi le record pour le nombre de plaintes déposées parmi tous les organismes gouvernementaux.

Il y a deux ans, la SCP avait le triste honneur d'être le plus important client du Commissariat. Elle avait cependant reçu des félicitations : près de 80 p. 100 des plaintes à son endroit n'étaient pas fondées; beaucoup portaient sur l'administration de sa politique interne sur l'assiduité et les congés et sur son programme de fonctions modifiées à l'intention des employés incapables à accomplir leur travail normal en raison d'une blessure ou d'une maladie.

Cette année, plus de la moitié des nouvelles plaintes visaient des recours inappropriés aux exceptions prévues par la Loi (les plaignants ont obtenu gain de cause dans la moitié des cas) et des délais de traitement (22 des 24 plaintes ont été jugées fondées).

Presque toutes les plaintes provenaient d'employés ontariens de la SCP impliqués dans des conflits de travail (surtout dans la région métropolitaine de Toronto et dans le sud de l'Ontario). Certains représentants officiels de la SCP en relations de travail estiment qu'il est fondamentalement injuste que les employés touchés par un conflit de travail puissent recourir à la Loi sur la protection des renseignements personnels pour obtenir des

La Direction des plaintes

Cette année n'a apporté aucune surprise. Le nombre des nouvelles plaintes a atteint le chiffre record de 1 579, soit une augmentation de 13 p. 100. Cependant, les enquêteurs ont fermé 1 440 dossiers au cours de l'année, soit presque deux fois plus que l'an dernier. De ce nombre, 590 plaintes étaient fondées, 757 plaintes ne l'étaient pas et 104 ont été abandonnées.

Les délais de traitement et les refus d'accès ont constitué 86 p. 100 du total des plaintes reçues. Pour se justifier, nombre d'institutions fédérales ont invoqué les compressions de personnel suscitées par la volonté du gouvernement de réduire les dépenses. Il en a résulté un service plus lent pour les demandeurs.

Performance des institutions

On retrouve là encore peu de surprises. Plus de 85 p. 100 des nouvelles plaintes mettaient en cause pratiquement les mêmes ministères que par les années précédentes : Service correctionnel Canada, Revenu Canada—Impôt, Emploi et Immigration Canada, la Société canadienne des postes, le Service canadien du renseignement de sécurité, la Gendarmerie royale du Canada, Revenu Canada—Douanes et Accise et la Défense nationale. Transport Canada et Santé et Bien-être social Canada s'ajoutent cette année à la liste.

Santé et Bien-être social Canada (SBSC)

Les nouvelles plaintes déposées à l'endroit de SBSC se sont chiffrées à 132 cette année (refus d'accès: 90; délais: 28; autres: 14) comparativement à 40 l'an dernier. La plupart portaient sur des renseignements détenus dans le cadre des programmes sur la sécurité du revenu (régime de pension du Canada, allocations familiales et sécurité de la vieillesse) lesquels tiennent des dossiers sur pratiquement l'ensemble de la population canadienne.

son consentement pour l'utilisation de ces derniers. Il y va de la survie de l'industrie. Le code n'est pas parfait: il n'existe pas de limites à la collecte (comme l'envisagent les lignes directrices de l'OCDE) et le mécanisme de surveillance n'est pas indépendant. Néanmoins, un tel effort mérite bien les applaudissements des consommateurs et des commissaires à la protection de la vie privée.

professions qui vont bien au-delà de ceux des membres immédiats de la CSA.

Association canadienne du marketing direct

Notre dernier rapport faisait également état de la décision de l'Association canadienne du marketing direct (ACMD) de développer son propre code de protection de la vie privée (l'ACMD siège aussi au sein du groupe de la CSA).

Cette association l'a fait. Le code qui a été rendu public en janvier 1993 est l'aboutissement de deux ans de recherches et de consultations auprès des consommateurs, de l'industrie et des experts en protection de la vie privée. Auparavant, l'ACMD offrait au consommateur la possibilité de faire rayer son nom des listes détenues par ses compagnies membres. Mais le nouveau code va plus loin. Il offre au consommateur la possibilité de contrôler le transfert des renseignements de marketing détenus à son sujet en lui permettant

- de refuser qu'on utilise son nom;
- de connaître l'origine des renseignements, de savoir quels renseignements sont détenus à son sujet et de demander que toute erreur soit corrigée;
- de contrôler l'utilisation subséquente de ces renseignements par des tiers;
- d'être rassuré au sujet des mesures de sécurité protégeant les renseignements;
- de bénéficier d'une protection plus rigoureuse pour les renseignements de nature délicate;
- de se plaindre à l'ACMD en cas de non-respect du code par un membre de l'Association.

Le code illustre bien ce qu'un engagement à l'égard d'une idée peut accomplir. Les membres de l'ACMD comprennent l'importance de conserver la confiance du consommateur, de lui offrir le contrôle des renseignements le concernant et d'obtenir

Code modèle de l'Association canadienne de normalisation

L'année dernière, nous avons signalé l'initiative prise par l'Association canadienne de normalisation (CSA) visant à développer un code d'éthique qui servirait de norme minimale de gestion des renseignements personnels pour les entreprises du secteur privé. Ce code modèle permettrait d'assurer une certaine protection de la vie privée sans avoir recours à une nouvelle loi.

La CSA a formé un comité dont le but est de développer, puis de promouvoir ce code modèle établi selon les lignes directrices de l'OCDE. Les membres du comité, y compris le Commissariat, proviennent des secteurs des finances, de l'assurance, du marketing direct, des télécommunications, de la technologie de l'information, des services publics, des agences d'évaluation du crédit, des consommateurs et des gouvernements fédéral et provinciaux.

Le travail se poursuit. Les groupes de travail du comité ont préparé des documents expliquant chacun des principes de l'OCDE en langage courant et relevé les questions qui doivent être résolues pour la mise en œuvre de ces principes. Ces documents doivent maintenant être révisés par un comité de rédaction, qui les fusionnera en une seule ébauche de code modèle. Le code devrait être soumis au comité plus tard cette année.

Un aspect important de tout code est le mécanisme de surveillance. Le comité prévoit faire des recommandations précises sur plusieurs options visant l'inscription ou la certification de codes propres à l'industrie.

Notre personnel a également contribué aux panels consultatifs de la CSA qui permettent au public d'étudier et de commenter les normes que propose l'Association. Les recommandations de ces panels aideront le comité à traduire les préoccupations, en matière de vie privée, d'une vaste gamme d'intérêts et de

d'exigences, en matière de couplage de données, applicables au secteur public, oblige les utilisateurs à vérifier l'exactitude des renseignements personnels avant le traitement et prévoit une vaste gamme de dommages-intérêts afin d'indemniser les personnes ayant subi une atteinte à leur vie privée.

Il comporte toutefois des omissions de taille : les organismes ont beaucoup de latitude lorsqu'il s'agit de déterminer ce qui constitue une demande et ils ont le droit d'exiger des frais pour le traitement des demandes d'accès, de correction et d'annotation. En outre, il semble que les auteurs d'actes criminels n'aient aucun droit d'accès ou de correction.

Le projet de loi ira bientôt à l'étape de la seconde lecture et devrait entrer en vigueur le 1^{er} juillet 1993.

a été produite par un sous-comité de la Commission de réforme du droit, formé de représentants des milieux universitaires, juridiques, des télécommunications, bancaires et commerciaux, ainsi que de la police et des médias.

La version préliminaire renferme les huit principes de l'OCDE et reflète, dans une large mesure, l'esprit de la plus récente directive préliminaire de la CE. Elle comporte une description détaillée de ce qui constitue des renseignements personnels et elle s'appliquera aux secteurs privé et public. Il y est aussi question de codes sectoriels, du couplage des données, du marketing direct, de numéros d'identification personnels et du flux transfrontier des données. Deux de ses points forts semblent être, premièrement, qu'elle prévoit des dispositions afin d'assurer que les personnes concernées consentent à l'utilisation et à la divulgation de leurs renseignements personnels et, deuxièmement, qu'elle donne aux personnes la possibilité de se retirer des activités reliées au marketing direct.

L'avenir du projet de loi est toutefois incertain, étant donné le retour de Hong Kong sous l'autorité de la Chine en 1997.

...et en Nouvelle-Zélande

La Nouvelle-Zélande s'est engagée dans le processus d'étude d'une loi générale sur la protection de la vie privée qui remplacerait divers textes législatifs ayant chacun une portée limitée. Le projet de loi stipule douze principes en matière de protection de la vie privée, soit un éventail plus complet que celui de l'OCDE ou de la directive de la CE. La Loi s'appliquera aux secteurs privé et public et elle traitera de sujets comme les codes d'éthique du secteur privé, les registres publics (les listes électorales, par exemple) et le couplage de données.

En vertu du projet de loi, le commissaire à la protection de la vie privée aurait le droit d'émettre en cas d'urgence des codes d'éthique. Le projet de loi énonce également un ensemble complet

Séance d'information sur la protection de la vie privée de l'OCDE

La technologie est généralement perçue comme un instrument de détérioration plutôt que de promotion de la vie privée. Mais, lors d'une réunion de l'Organisation de coopération et de développement économique (OCDE) en novembre 1992, les participants ont été invités à regarder l'envers de la médaille, c'est-à-dire à examiner les possibilités que présente la technologie pour la protection des renseignements personnels. L'OCDE a invité plusieurs spécialistes à renseigner les participants gouvernementaux sur l'utilisation de nouvelles technologies et nouveaux processus pour la protection des données personnelles informatisées.

Certaines de ces nouvelles techniques sont, entre autres, le chiffrement des données (codage), les systèmes validés (conçus pour satisfaire à des objectifs de sécurité bien précis), les signatures cachées, l'encaisse électronique (vérification des opérations financières sans identifier la personne concernée) et les réseaux qui permettent la transmission entre des partenaires sans qu'ils soient « observés ». Il serait étonnant que l'une de ces techniques se révèle à toute épreuve, mais ces réunions constituent une étape importante en vue de l'intégration de mécanismes de contrôle aux systèmes en place. Le groupe compte se réunir de nouveau.

L'OCDE a également adopté ses nouvelles lignes directrices régissant les systèmes de sécurité de l'information. Celles-ci devraient être publiées bientôt.

La protection de la vie privée à Hong Kong...

Le gouvernement de Hong Kong a récemment publié un document de travail examinant les mesures de protection de la vie privée en vigueur dans cette colonie de la Couronne, décrivant des dispositions législatives en la matière. La version préliminaire

des finances. Les milieux d'affaires ont cerné plusieurs problèmes : la restriction touchant le flux de renseignements personnels vers les pays sans protection « appropriée » qui ne font pas partie de la CE ; la nécessité d'obtenir le consentement exprès de la personne concernée avant le traitement ou le transfert des données ; les obligations « inutilement lourdes » d'informer les autorités chargées de la protection des renseignements personnels ; et le peu de souplesse dont disposent les États membres dans l'utilisation des divers genres de règlements ou de codes pour la mise en œuvre des principes de protection des données.

L'offensive des milieux d'affaires a eu un certain effet et, en octobre 1992, la CE a émis une directive révisée. Cette dernière exige encore qu'une protection « appropriée » soit prévue dans les pays autres que ceux de la CE et qui reçoivent des données relatives aux résidents de la CE. En outre, cette version ne fait plus de distinction entre les secteurs privé et public—Ils sont soumis aux mêmes règles. Elle est cependant plus souple. Ainsi, les transferts de données sont maintenant permis sous réserve que la personne concernée y consent, les données sont nécessaires dans le cadre de l'exécution d'un contrat entre la personne concernée et le contrôleur (sur avis donné à la personne concernée), et pour des raisons importantes d'intérêt public or d'intérêt crucial de la personne concernée.

En vertu de la version révisée de la directive, les États membres de la CE pourront aussi tenir compte du genre de données, de la raison du traitement, de codes sectoriels et, des dispositions législatives et même des « règles de conduite » lorsqu'ils devront évaluer le caractère « pertinent » de la protection assurée aux données personnelles dans les pays qui ne sont pas membres de la CE.

Il est difficile de prévoir si la mosaïque de lois du secteur public et de codes du secteur privé (ou d'énoncés de bonne intention) qui existe au Canada sera à la hauteur.

L'année dernière, la directive de la CE a été prise à partie par les milieux d'affaires, en particulier les secteurs du marketing direct et

l'Amérique du Nord.
provenance de la Communauté vers d'autres pays—en particulier, très strictes en matière de flux de données personnelles, en canadiens quant aux retombées possibles de règles européennes avaient mis en garde les gouvernements et les milieux d'affaires la Communauté européenne (CE). Certains rapports antérieurs projet de directive sur la protection des données personnelles de La meilleure preuve de ce qui précède nous est fournie par le au-delà des frontières nationales ou régionales.

Bien entendu, les développements dans le domaine de la protection de la vie privée peuvent avoir des répercussions bien

A l'étranger: Projet de directive de la Communauté européenne

organismes réticents.
ordonnances—le commissaire pourra imposer des délais aux des avantages indéniables à pouvoir prendre des des délais; les examens devront être achevés en 90 jours. Il y a recherche. Néanmoins, le commissaire lui-même devra respecter elle aura un mandat précis en matière d'éducation et de Cabinet pour évaluer la validité des demandes d'exemption. Il ou commissaire pourrait avoir accès aux documents confidentiels du Contrairement à notre organisme à l'échelon fédéral, le médiation et en cas d'échec, la prise d'ordonnances exécutoires. Les plaintes seront traitées par un commissaire—en partie protecteur du citoyen et en partie tribunal, permettant ainsi la

printemps de 1995.
professionnels autoréglémentés seraient couverts d'ici au les municipalités. En vertu d'autres modifications, les organismes locaux comme les conseils scolaires, les hôpitaux et pour que ses dispositions s'étendent, en octobre 1994, aux

Des dispositions précises s'appliquent aux agences d'évaluation du crédit, qui doivent s'inscrire auprès de la Commission provinciale d'accès à l'information et signaler leurs activités dans les journaux. Le projet de loi prévoit des amendes, pour l'observation de la loi, allant de 1 000 \$ à 10 000 \$ selon la gravité d'infraction.

La Commission d'accès de l'information du Québec jouera un rôle primordial dans l'administration de la loi. Elle fera enquête lorsque des plaintes sont déposées et rendra des décisions (les questions de droit et de compétence pourront être portées en appel devant les tribunaux). Elle aura aussi un mandat d'éducation et elle encouragera et aidera les entreprises à élaborer des codes d'éthique internes concernant la vie privée.

Une commission législative a tenu des audiences publiques et révisé maintenant le projet de loi; elle envisage d'apporter des modifications précises.

Au moins une question demeure sans réponse : est-ce que la loi s'appliquera aux entreprises faisant l'objet d'une réglementation fédérale, comme les banques, les transports et les communications? Dans l'affirmative, est-ce que ces secteurs offriront le même niveau de protection de la vie privée aux autres Canadiens?

Colombie-Britannique

En juin 1993, le Parlement de la Colombie-Britannique a adopté sa première loi, intitulée *Freedom of Information and Protection of Privacy Act*, sur la liberté d'accès à l'information et la protection des renseignements personnels.

La loi (qui entrera en vigueur en octobre 1993) ressemble beaucoup aux autres lois provinciales et s'appliquera aux organismes provinciaux de la Colombie-Britannique. Cependant, avant même d'entrer en vigueur, elle est en voie d'être modifiée

Les lecteurs assidus de ces rapports savent que le Commissariat suit la situation en matière de protection de la vie privée dans notre monde de plus en plus interrelié. Voici les progrès tant au Canada qu'à l'étranger.

À l'échelon provincial : le Québec

Le gouvernement du Québec a déposé, en décembre 1992, le projet de loi 68, qui étend l'application des dispositions en matière de protection de la vie privée au secteur privé.

Si la loi est adoptée, elle constituera la première loi en Amérique du Nord à réglementer la collecte, l'utilisation et la communication de renseignements personnels sur les clients et les employés.

La loi exigerait qu'une entreprise recueille seulement à des fins précises les renseignements personnels. L'entreprise ne pourrait refuser à un client des biens ou des services si le client refuse de fournir des renseignements personnels à moins que les détails soient exigés en vertu de la loi ou pour remplir des obligations contractuelles.

La loi exigerait également qu'une entreprise signale à ses clients les renseignements détenus à leur sujet, que les données soient précises, à jour et complètes et que l'entreprise obtienne le consentement du sujet pour toute communication des renseignements à des tiers lorsque la communication ne correspond pas au but dans lequel les renseignements ont été recueillis à l'origine (sauf lorsque cela est prévu dans la loi).

Le consommateur pourra choisir de ne plus être ciblé par le télémarketing ou le publipostage et savoir où l'entreprise a obtenu les renseignements personnels. L'entreprise doit avoir pris les mesures de sécurité appropriées pour protéger la confidentialité des renseignements personnels.

pendant des siècles, et cela, au nom du sport pratiqué par des athlètes masculins et féminins.

Dépistage génétique

Le Commissariat continue de surveiller les développements rapides dans le domaine du dépistage génétique et leurs incidences sur la vie privée. Notre rapport de 1992, intitulé *Le dépistage génétique et la vie privée*, a été accueilli favorablement à l'échelon national et international, mais les préoccupations relatives à la vie privée restent à la traîne d'autres questions d'intérêt public. Le caractère urgent des dangers du dépistage génétique non réglementé risque de passer inaperçu.

La technologie génétique ne nous laissera pas reprendre notre souffle. Les découvertes génétiques surviennent de plus en plus rapidement. Les chercheurs et les biotechnologues continueront de mettre au point de nouveaux tests de dépistage génétique, moins coûteux et plus précis, en vue d'identifier des traits physiques ou de comportement. Certains traits, révélés à l'employeur, à l'assureur et aux gouvernements, stigmatiseront presque certainement les personnes ou accéléreront la discrimination à leur égard fondée simplement sur leurs gènes.

Dans l'intervalle, nous approchons du moment où nous perdrons le contrôle de notre propre information génétique—qui constitue notre essence même. Le Commissaire exhorte le Parlement à se pencher sur cette question avant que ne s'en suive une mêlée générale en génétique, dépassant les plus noires visions d'Orwell.

Employés du secteur des transports

Un troisième grand point, en ce qui a trait à la question du dépistage antidrogue, touche le secteur des transports. Au moment d'aller sous presse, il semble que la législation en matière de dépistage antidrogue visant les titulaires de postes comportant des risques pour la sécurité dans les transports ne sera probablement pas déposée avant l'ajournement d'été au Parlement.

Nous avons exprimé plusieurs fois notre inquiétude au sujet du programme de dépistage proposé dans les transports, et nous continuons de croire qu'il s'agit d'une mesure excessive. En même temps, ce programme sacrifie inutilement des droits à la vie privée qui ont été durement gagnés. La décision du ministre des Transports de ne pas procéder à un dépistage au hasard est le seul point que nous jugeons positif. Quoi qu'il en soit, au chapitre de la protection de la vie privée, le programme de dépistage prévu demeure discutabile sous plusieurs autres aspects.

Dépistage chez les athlètes

Nous demeurons également au fait des développements du dépistage antidrogue dans les sports. Les athlètes ont eux aussi des droits fondamentaux, y compris le droit à la vie privée. Peut-être que les programmes de dépistage contribueront à rendre les compétitions sportives plus loyales, mais à quel prix? Nous nous préoccupons en particulier de l'intérêt montré par certains répondants dans un récent questionnaire du Centre canadien sur le dopage sportif, (ils ont identifié le dépistage mené au moyen d'analyses sanguines comme représentant une activité appropriée du Centre). Les analyses d'urine sont, à coup sûr, une violation de la vie privée, mais du moins elles n'exigent pas de pénétrer dans le corps d'une personne pour y prélever des liquides organiques comme c'est le cas avec les analyses sanguines. Il est terrible de penser que certaines personnes sont prêtes à envisager de violer l'intégrité de l'être humain, une intégrité protégée par la loi

Dépistage chez les détenus et les libérés conditionnels

La Loi régissant le système correctionnel et la mise en liberté sous condition, qui est entrée en vigueur en novembre 1992, instaure une gamme étendue de programmes de dépistage antidrogue touchant les détenus et les libérés conditionnels. Les motifs fournis pour soumettre les détenus et les libérés conditionnels diffèrent de ceux qui ont été invoqués dans d'autres dépistages. Il paraît que le commerce de la drogue dans les prisons suscite de la violence et de la coercition. Le dépistage antidrogue, avance-t-on, peut entraîner une diminution de la demande et, partant, une diminution de ce climat de violence.

Le Commissariat n'a pas d'objection à l'utilisation de mesures raisonnables susceptibles de réduire la violence dans les prisons. Néanmoins, rien n'indique encore que le dépistage antidrogue réussira à cet égard. S'il réussit, cette atteinte à la vie privée peut être justifiée. Autrement, nous espérons que le Solliciteur général du Canada sera assez ouvert d'esprit pour remettre le programme en question.

Le dépistage antidrogue dans les prisons peut donner lieu à un danger particulièrement grave. Pour éviter d'être dépistés, les consommateurs de drogue pourraient être tentés d'abandonner les drogues qui restent longtemps décelables dans l'organisme (comme la marijuana) au profit de celles qui disparaissent plus rapidement. Par le fait même, ils abandonneront peut-être une drogue qu'ils peuvent fumer pour utiliser une drogue administrée généralement par injection. Compte tenu de la rareté des seringues (et des produits de nettoyage des seringues) dans les prisons, ces changements d'habitude pourraient accroître considérablement les risques d'infection par le VIH. Si le programme mène finalement à une augmentation des risques d'infection par le VIH, alors il apportera un argument de plus contre le dépistage antidrogue, même si la question n'intéresse pas strictement la vie privée.

armées quelle drogue ils ont consommée au cours du dernier mois :

3 diraient du LSD
5 diraient de la cocaïne
25 diraient de la marijuana
780 diraient de l'alcool.

S'il existe des problèmes de sécurité liés à la consommation des drogues au sein des Forces canadiennes, ils découlent sûrement plus de la consommation d'alcool que des drogues illégales.

Malgré cela, ce sont ces dernières qui sont presque

exclusivement visées par la politique de dépistage antidrogue.

L'étude de 1989 a clairement révélé que la consommation de

drogues illégales dans les Forces canadiennes n'est pas d'une

ampleur telle qu'elle justifie une intrusion massive dans les corps

des militaires par le dépistage antidrogue. Nous avons fait part,

sans grand résultat, de nos réserves aux hauts gradés du

ministère de la Défense nationale et avons écrit à ce sujet au

Chef d'état-major de la Défense. Le Commissaire compte

poursuivre le sujet.

Un test anonyme effectué dans 15 endroits au Canada et en Allemagne le 8 décembre 1992 a permis de recueillir plus de 5 500 échantillons d'urine. Ces échantillons ont été analysés pour détecter les canabinoïdes, soit la marijuana, la cocaïne, les opiacés, les amphétamines et le PCP.

Les résultats du test anonyme (qui ne sont pas, entièrement comparables aux résultats du sondage précédent), viennent à l'appui de la position adoptée par le Commissariat à l'effet que les taux de consommation de drogues sont très peu élevés et que le programme de dépistage massif lancé pour les détecter est une intrusion injustifiée.

décalage horaire à un certain moment au cours du dernier mois ou de la dernière semaine. Cette information ne renseigne nullement sur l'état du pilote au moment du dépistage.

Ce n'est pas que le Commissariat soit insensible aux préoccupations en matière de sécurité du public. Il admet volontiers que certaines circonstances peuvent justifier l'empêchement sur la vie privée. La loi autorisant les tests d'ivresse montre en est un exemple. Mais le dépistage antidrogue n'est pas justifié à ce titre. Au contraire, il représente un nouveau genre de violation importante du corps humain, parrainée par l'État. Est-il nécessaire de rappeler que la loi a un tel respect pour l'intégrité du corps humain qu'elle prévoit même que les personnes accusées de meurtre ne peuvent être soumises contre leur gré au prélèvement de substances organiques à des fins médico-légales.

Bref, le dépistage antidrogue constitue une violation grave qui ne procure en contrepartie aucun avantage tangible.

Les programmes de dépistage des Forces canadiennes

Le programme de dépistage antidrogue maintenant en vigueur dans les Forces canadiennes nous préoccupe tout particulièrement. Dans notre rapport *Le dépistage antidrogue et la vie privée*, publié en 1991, nous nous interrogeons sur la nécessité d'astreindre les militaires à ces tests. Nous nous appuyons pour cela sur les résultats d'une enquête menée en 1989 auprès des militaires, qui avait clairement démontré que l'alcool, et non pas les drogues, était le plus grand facteur potentiel de risque dans les Forces canadiennes. La façon la plus simple d'expliquer les résultats de l'enquête est la suivante : si, en se fondant sur l'enquête de 1989, on demandait à 1 000 membres des forces

Le dossier de la biotechnologie : quoi de neuf?

Cette année, deux événements importants sont survenus à l'échelon fédéral. Le premier, en mai 1992, a été l'entrée en vigueur du règlement autorisant un vaste éventail de programmes de dépistage antidrogue dans les Forces canadiennes. En novembre, la *Loi régissant le système correctionnel et la mise en liberté sous conditions* est entrée en vigueur. Elle autorise également une vaste gamme de programmes de dépistage touchant les détenus et les contrevenants mis en liberté conditionnelle.

Le dépistage antidrogue ne cesse de préoccuper le Commissariat. La plus grande menace à la sécurité du public et du milieu de travail est, en effet, l'alcool et non les drogues. Pourtant, le gouvernement a continué de poursuivre le dépistage antidrogue.

Le dépistage antidrogue (analyse d'urine) ne permet pas de déterminer si les facultés d'un sujet sont affaiblies. Même l'alcootest est une mesure imprécise et la limite légale est fixée arbitrairement. Le dépistage antidrogue ne peut que déterminer si la personne a consommé une drogue donnée dans le passé. Il ne renseigne pas sur la quantité consommée, le moment exact de la consommation (au mieux, à l'intérieur d'un certain nombre de jours et, au pire, de semaines), ou si la drogue a provoqué un affaiblissement des facultés au moment de la consommation. Plus important encore, le dépistage ne peut pas établir si les facultés du sujet sont affaiblies **maintenant**. Le dépistage antidrogue ne permet donc pas d'obtenir la seule information qui soit vraiment pertinente, à savoir si la personne a les facultés affaiblies au moment présent.

En termes simples, le dépistage antidrogue ne signalera pas aux passagers aériens si leur pilote n'est pas en état de tenir les commandes. Ils sauront seulement s'il a consommé une drogue dans le passé, information tout aussi inutile que d'apprendre que leur pilote a consommé de l'alcool, a souffert de la grippe ou du

La Cour a conclu que les documents appartenaient effectivement au médecin et elle a également affirmé que le médecin a le devoir de protéger le caractère confidentiel du dossier médical d'un patient, à moins que ce dernier ou la loi ne l'autorise à agir autrement. Cependant, la Cour a précisé très clairement que la relation médecin-patient en est une de confiance et que l'information qu'un patient révèle à un médecin demeure, fondamentalement, sienne.

La Cour a fait observer que l'intérêt bénéfique de nature fiduciaire que détient la patiente à l'égard de cette information indique qu'elle devrait, en règle générale, avoir le droit d'accéder à l'information et que le médecin devrait avoir l'obligation correspondante de lui assurer ce droit.

Il ne s'agit pas d'un droit absolu. La Cour a reconnu qu'un médecin pourrait avoir des raisons de croire qu'il ne serait pas dans le meilleur intérêt d'un patient d'avoir accès à certains documents. Toutefois, c'est ainsi au médecin qu'il incomberait de justifier son refus à un patient.

Cette décision a une incidence limitée dans l'immédiat puisqu'elle s'applique seulement aux compétences où il n'existe pas de loi touchant le droit d'accès des patients. Elle n'en constitue pas moins, de la part du plus haut tribunal au pays, une réaffirmation importante du droit de propriété qu'ont les personnes à l'égard de leurs renseignements personnels.

et Immigration Canada attribue des NAS aux nouveaux-nés de l'I-P-E.

Voici le commentaire en question : «...la province n'a pas le droit de recevoir, de la part du gouvernement du Canada, des renseignements sur les numéros d'assurance sociale de personnes sans le consentement des personnes concernées, étant donné qu'elle ne satisfait pas aux dispositions du paragraphe 8 (2) de la Loi sur la protection des renseignements personnels» (Traduction).

Le Commissaire a examiné la décision qui étaye ses doutes sur la validité de l'entente de 1970 (conclue bien avant que la Loi n'entre en vigueur). Il a donc écrit de nouveau à EIC, demandant cette fois au ministère d'interrompre l'attribution de NAS dans le cadre de cette vieille entente. EIC et Santé et Bien-être social Canada se sont tous deux engagés à recommander à l'Île-du-Prince-Édouard de mettre fin à l'utilisation du NAS en guise de numéro d'identité pour son régime de soins de santé et ils ont entrepris d'aider la province à adopter, à cette fin, son propre système d'identification. EIC attendra toutefois le résultat de l'appel interjeté par les parents.

Une patiente gagne accès à son dossier médical

Dans une autre affaire, la Cour suprême du Canada a déterminé qu'une résidente du Nouveau-Brunswick avait le droit de consulter tous les documents versés dans son dossier médical, et non pas seulement ceux créés par son médecin traitant actuel.

Le médecin avait fourni des copies de tous les documents qu'elle avait préparé, mais elle avait refusé de permettre à la patiente d'examiner ceux qui avaient été créés par d'autres médecins. Le médecin soutenait que cela aurait compromis l'éthique puisque ces documents étaient la propriété de quelqu'un d'autre.

renseignements personnels de Jean. Le Commissaire a demandé à la Cour de se pencher sur la distinction existant entre une source de renseignements confidentielle qui fournit des renseignements dans le cadre de l'application de la loi et un témoin dont le témoignage est entendu à la faveur d'un processus administratif. La Cour sera également priée d'évaluer le tort qui pourrait survenir de la divulgation une fois ce genre d'enquête administrative terminée.

Aucune date n'a encore été fixée pour l'audience.

Au cours de la dernière année, les tribunaux ont rendu des décisions dans deux causes intéressant la protection de la vie privée.

Le premier cas avait trait au fait que l'Île-du-Prince-Édouard exigeait qu'un numéro d'assurance sociale (NAS) soit attribué à un nouveau-né, comme le signalait notre dernier rapport annuel.

Pour résumer, un couple a refusé de faire une demande de NAS pour son nouveau-né et s'est vu refuser, par la suite, les demandes de remboursement de frais médicaux de l'enfant, parce que celle-ci n'avait pas de NAS (le numéro d'identité pour le régime provincial de soins de santé). Les parents ont soutenu qu'obliger quelqu'un à avoir un NAS comme condition d'admissibilité au paiement des services médicaux violait la *Charte*, ainsi que le droit de cette personne à l'égalité devant la loi et ses attentes légitimes à une protection de sa vie privée.

Le tribunal a réfuté chacun des arguments des parents. Néanmoins, le Commissariat a été des plus intéressés par le commentaire qu'a émis le tribunal sur la *Loi sur la protection des renseignements personnels* et son application à une entente fédérale-provinciale conclue en 1970 en vertu de laquelle Emploi

Le Commissaire à la protection de la vie privée et la Société canadienne des postes

Pour la première fois depuis l'avènement de la Loi, il y a 10 ans, le Commissaire à la protection de la vie privée a référé à la Cour fédérale un cas de refus d'accès à des renseignements personnels.

Le Commissaire a demandé à la Cour de déterminer si un plaignant a le droit de connaître l'identité d'une personne qui a témoigné contre lui dans l'audition d'un grief, le grief ayant été fondé sur ce témoignage.

À l'origine, la Société canadienne des postes avait refusé de communiquer à l'homme le nom et la teneur du témoignage du témoin en faisant valoir que ces renseignements avaient été «obtenus ou préparés au cours d'une enquête» et que leur communication nuirait au déroulement d'une enquête [alinéa 22 (1) b]. L'homme a alors porté plainte auprès du Commissaire. Durant l'enquête, la Société canadienne des postes a accepté de communiquer le témoignage. Cependant, elle en avait enlevé tout détail qui aurait pu révéler l'identité du témoin et avait maintenu son refus de divulguer le nom de ce dernier.

La Société a soutenu que la communication du nom du témoin «nuirait à l'application de toute loi» étant donné que l'information avait été préparée pendant une enquête et que cela permettrait de remonter à une source de renseignements confidentielle. Elle a aussi maintenu qu'en révélant l'identité du témoin, elle violerait la disposition de la Loi interdisant la communication de renseignements sur un autre individu que celui qui fait la demande (article 26).

La Loi sur la protection des renseignements personnels comprend, dans les renseignements personnels, «les idées ou opinions d'autrui sur soi». Autrement dit, si Marie fait des commentaires sur Jean, ces commentaires constituent les

valable à l'intérieur d'une plage de +/- 1,8 point soit, 19 fois sur 20. L'étude servira de point de référence lorsque des études ultérieures seront menées pour déterminer l'évolution de la question de la vie privée.

Le Commissariat n'aurait pu réaliser seul un sondage de cette envergure et de cette rigueur et il en va probablement de même pour les autres associés fédéraux. Le Commissaire remercie la firme Les Associés de recherche Ekos Inc. pour la qualité des analyses et les nombreuses heures supplémentaires consacrées au projet, Stentor politiques publiques Télécom Inc. pour l'initiative, les fonds, et le travail fourni par son personnel, et Communications Canada pour les contributions apportées par le personnel des politiques. Il aurait été impossible de concrétiser le projet sans leur participation.

est rassuré. Ce besoin de participer au processus et d'être en contrôle est manifeste dans les résultats suivants.

- 81 p. 100 sont fermement convaincus qu'on doit les prévenir à l'avance lorsqu'on recueille des renseignements à leur sujet;
- 83 p. 100 sont fermement convaincus qu'un organisme doit obtenir leur consentement avant de transmettre à un autre organisme des renseignements à leur sujet;
- 87 p. 100 sont bien d'accord que, lorsque de l'information est recueillie à leur sujet, ils devraient être informés de l'utilisation qui en sera faite;

- 72 p. 100 des répondants ont jugé extrêmement important de pouvoir contrôler à qui va l'information;

- 67 p. 100 jugent extrêmement important de pouvoir contrôler la teneur des renseignements recueillis à leur sujet.

Le sondage (intitulé *La vie privée exposée*) a révélé que les répondants veulent avec insistance que des mesures soient prises. Les répondants étaient prêts à envisager des approches innovatrices comme les partenariats entre le gouvernement et l'entreprise—et à assumer eux-mêmes des responsabilités—mais le sondage a clairement montré que l'autoréglementation par les entreprises (le statu quo) était l'option la moins acceptable (26 p. 100). Une participation active du gouvernement était l'option la plus retenue.

Le sondage a été mené par la firme Les Associés de recherche Ekos Inc. d'Ottawa pour le Commissariat à la protection de la vie privée, la Banque Amex du Canada, l'Association des banquiers canadiens, Consommation et Affaires commerciales Canada, Communications Canada, Equifax Canada Inc., Statistique Canada et Stentor politiques publiques Télécom Inc. Il a porté sur 3 000 ménages canadiens; un échantillonnage de cette taille est

La vie privée exposée : sondage canadien sur la vie privée

Pour la première fois dans ses dix années d'existence, le Commissariat possède une analyse fiable des attentes, des connaissances et des craintes des Canadiens à l'égard de la vie privée—qu'ils jugent assaillie.

Les résultats de cette première étude d'envergure étaient attendus depuis longtemps. L'étude confirme de façon spectaculaire que la population est consciente des dangers que posent les changements technologiques, commerciaux et sociaux.

L'étude a révélé que 92 p. 100 des Canadiens ressentent une certaine préoccupation au sujet de la vie privée—52 p. 100 étaient «très inquiets»—cela est comparable à la très grande préoccupation au sujet de l'environnement (52 p. 100) et de l'emploi (56 p. 100) et aux inquiétudes ressenties en matière d'unité nationale (31 p. 100).

La plupart des Canadiens (60 p. 100) estiment que leur vie privée est moins respectée qu'elle ne l'était il y a dix ans et 40 p. 100 croient fermement qu'il y a eu une érosion de la vie privée. Quatre répondants sur cinq jugent que l'ordonnateur diminue la vie privée et 54 p. 100 ont de vives préoccupations au sujet du recoupement de l'information personnelle d'une base de données à l'autre.

Le résultat peut-être le plus surprenant pour le Commissariat à la protection de la vie privée est que, qu'ils aient jamais lu ou non une loi sur la protection de la vie privée ou entendu parler du Commissariat à la protection de la vie privée (cas peu fréquents, comme le montre le sondage), les Canadiens ont relevé les éléments fondamentaux de la protection de la vie privée : la connaissance, le contrôle et le consentement.

L'une des tendances clés révélée par le sondage est que, plus un répondant connaît bien le processus et se sent en contrôle, plus il

Parlement à profiter de l'occasion qui s'offrait pour ébaucher de nouveaux règlements qui protégeraient la vie privée dans le monde bancaire. Le Comité a réagi rapidement et il a ébauché des règlements avec l'aide de M. David Flaherty, professeur à l'Université Western Ontario. Ces règlements reposent sur des dispositions de la *Loi sur la protection de la vie privée*, adaptées au domaine bancaire.

Tel que promis, le Commissaire a été invité à comparaître de nouveau devant le Comité en décembre. Il a réitéré son soutien ferme à l'enchâssement, dans la loi, de normes fondamentales en matière de protection de la vie privée. De même, il a soutenu qu'aucun plan de protection de la vie privée n'obtiendrait la confiance du public sans qu'existe un mécanisme indépendant de résolution des conflits, doté du pouvoir d'enquêter sur les plaintes et d'examiner tant les informations détenues que les pratiques de gestion des informations des institutions financières. Jusqu'à ce jour, le comité sénatorial n'a pas publié son rapport final.

L'Association des banquiers canadiens est à la tête d'un groupe de pression assez important du secteur privé qui préconise une approche entièrement autoréglementée. Le Commissaire n'est pas fervent de l'intervention gouvernementale en soi, mais il continue néanmoins d'estimer que des normes communes et un droit de regard indépendant sont nécessaires pour assurer l'équité et la transparence dans le domaine bancaire.

cadre de son processus d'administration des employés. Les résultats seront certainement intéressants pour la bureaucratie et le Parlement. Dans l'intervalle, le Commissaire reconnaît que Revenu Canada a répondu avec diligence à ses préoccupations.

Deux autres modifications préoccupaient aussi le Commissaire, soit la modification de l'article 241 de la *Loi sur l'impôt sur le revenu*, qui prévoit qu'un fonctionnaire «pourrait» donner accès à l'information des contribuables aux fins de l'article 45 de la *Loi sur la protection des renseignements personnels* (même énoncé pour l'article 295 de la *Loi sur la taxe d'accise*). Ces dispositions auraient pu être interprétées comme accordant aux fonctionnaires du ministère la latitude de refuser de divulguer des renseignements de contribuables au personnel du Commissariat au cours d'une enquête sur une plainte.

Revenu Canada a reconnu que ces articles devraient être interprétés uniquement comme permettant aux fonctionnaires du ministère de permettre au Commissaire à la protection de la vie privée d'exécuter ses fonctions sans que Revenu Canada entreigne les articles 241 de la *Loi sur l'impôt sur le revenu* ou 295 de la *Loi sur la taxe d'accise*.

La vie privée et les institutions financières

Le Commissaire avait signalé l'année dernière qu'une grande étape avait été franchie avec l'introduction de deux documents législatifs—un projet de loi traitant des banques et institutions financières et une nouvelle loi sur les télécommunications. Comme nous l'avons déjà signalé, des initiatives récentes laissent davantage espérer que la vie privée sera adéquatement protégée dans le domaine des télécommunications. Il en va autrement dans le domaine bancaire où les dispositions semblent accrocher. En avril 1992, le Commissaire a comparu devant le Comité sénatorial permanent des banques et du commerce pour inciter le

finances de la Chambre des communes. Les modifications ont été au départ repoussées par le comité, mais elles ont été rétablies à l'étape de rapport par le gouvernement.

Dans sa correspondance adressée au Commissaire à la protection de la vie privée et au Comité, le ministère a reconnu que les propositions modifient fondamentalement les dispositions en matière de confidentialité, mais il a soutenu

qu'il est de notre devoir de veiller à ce que les employés de l'impôt sur le revenu se comportent d'une façon qui sied aux personnes ayant accès privilégié au système fiscal. La plupart des employés ont un tel comportement, mais, il serait injuste pour les autres contribuables qu'un employé de l'impôt sur le revenu ayant abusé du système ou ayant fait preuve d'incompétence soit à l'abri des mesures disciplinaires habituelles, simplement parce que la preuve pertinente dans le domaine fiscal ne pourrait pas être utilisée ou obtenue. (Traduction)

Le ministère a soutenu que les modifications renforcent la protection de la vie privée puisque l'information du contribuable pourrait être utilisée **seulement** si elle est **pertinente** à la supervision, à l'évaluation et à la discipline. En outre, le ministère a proposé d'émettre des lignes directrices pour répondre aux objections du Commissaire à la protection de la vie privée. Ses représentants ont déclaré que le Commissaire et les représentants du syndicat seraient consultés avant l'achèvement et la mise en œuvre des lignes directrices.

Le Commissaire a bien accueilli l'offre que lui a présentée le ministre, visant à élaborer un ensemble de mesures de protection mutuellement acceptables de concert avec les syndicats de la fonction publique concernés. C'est la première fois que le Commissariat aura travaillé directement avec un ministère à l'amélioration des aspects de protection de la vie privée dans le

Certaines occupations et professions exigent souvent de leurs membres des normes différentes ou plus poussées de comportement; cependant, le Commissaire estimait que le niveau d'intégrité souhaité par l'impôt pourrait être atteint sans la mise en œuvre de mesures si vastes.

Ainsi, le ministère pourrait établir des critères rigoureux en vertu desquels la direction pourrait examiner les déclarations d'impôt sur le revenu d'un employé. Il pourrait définir des motifs raisonnables afin d'éviter la consultation « au hasard » des dossiers personnels et de nature délicate des employés.

En outre, le ministère pourrait établir un protocole autorisant les hauts fonctionnaires seulement (et non les surveillants ou les employés du personnel) à examiner les dossiers des employés et à déterminer s'il y a lieu d'en divulguer le contenu aux fins d'utilisation par le personnel. Revenu Canada ne devrait pas envisager un tel examen et une telle divulgation à des fins de supervision et d'évaluation routinières, mais bien uniquement pour des « motifs » précisés dans la loi.

Dans le meilleur des cas, les propositions actuelles constituent une dérogation aux droits déjà existants en matière de vie privée sans qu'une protection correspondante soit appliquée aux intérêts des employés. De telles mesures ne devraient pas être prises à la légère, sans un débat public complet et ouvert. Elles pourraient susciter la création d'une sous-classe de citoyens, du point de vue de la vie privée, dont les préoccupations légitimes sont tout aussi importantes que l'intégrité du programme fiscal. La confidentialité des dossiers des citoyens est une question d'importance primordiale pour les employés de l'impôt. Tout système qui diminuerait la protection de la vie privée exige des mesures de sécurité rigoureuses. Un équilibre doit être atteint.

Ce manque apparent d'équilibre entre des intérêts concurrents n'est pas passé inaperçu auprès des membres du Comité des

renseignements fournis par le contribuable afin de superviser, d'évaluer ou de discipliner un employé du ministère.

Le Commissaire a soulevé deux questions importantes à ce sujet. Tout d'abord, ils font des employés d'impôt une nouvelle classe d'employés fédéraux, soumis à la surveillance et à des contrôles différents de ceux qu'emploie le gouvernement à l'égard des autres employés. Enfin, ils réduisent les droits actuels en matière de confidentialité de tous les contribuables puisqu'ils servent à des dossiers de ces derniers pour servir à des poursuites sans lien avec le processus de l'impôt sur le revenu.

Toutefois, dans le dernier cas, des mesures de protection ont été incluses afin de protéger la confidentialité des renseignements du contribuable durant des poursuites légales. On trouve au nombre de ces mesures la tenue à huis clos d'audiences, l'interdiction de publication de l'information, la non-divulgateion de l'identité du contribuable et le dépôt sous scellés des dossiers d'instance. Une telle utilisation de leurs dossiers pourrait néanmoins surprendre et inquiéter nombre de contribuables. Le Commissaire a recommandé que Revenu Canada sensibilise les contribuables à la modification avant de mettre en œuvre le système.

La première proposition, visant à désigner les employés de Revenu Canada comme une nouvelle classe d'employés, est une question encore plus préoccupante. Le Commissaire reconnaît le besoin d'assurer l'intégrité du système fiscal, mais il estime que les propositions, dans leur version préliminaire, sont d'une application trop vaste et pourraient compromettre la vie privée de l'employé. Les propositions pourraient être interprétées comme donnant à un surveillant le droit arbitraire de consulter à son gré la déclaration d'impôt d'un employé. Ainsi, par exemple, un employé de Revenu Canada participant à des procédures de grief contre un surveillant (sur des questions non liées à la perception de l'impôt sur le revenu), pourrait voir sa déclaration d'impôt utilisée par le surveillant pour le menacer ou l'intimider.

évidents. Tout d'abord, elle permet à l'industrie de se doter d'un cadre de travail en matière de protection de la vie privée qui est adapté à ses propres besoins. Deuxièmement, elle fournit une solution qui va au-delà des divers champs de compétence—tous les intervenants peuvent jouer un rôle, qu'ils proviennent du secteur privé ou public, ou qu'ils soient réglementés à l'échelon provincial ou fédéral. Troisièmement, le financement proviendra des secteurs privé et public.

Deux organismes joueront un rôle-clé dans l'approche de partenariat : la Canadian Telecommunication Privacy Foundation et le Canadian Telecommunications Privacy Council. La Fondation rassemblera tous les intervenants; le Conseil (représentant l'industrie et les consommateurs) recevra et arbitra les plaintes.

Toutefois, cette approche repose sur peu de fondements juridiques précis et n'établit pas de mécanisme indépendant de résolution des conflits—deux éléments essentiels à une adoption sans réserve de l'approche par le Commissaire à la protection de la vie privée. Néanmoins, si l'industrie l'adopte, cette approche pourrait constituer un cadre de travail satisfaisant dans le domaine de la protection de la vie privée. Le ministre des Communications est disposé à envisager une solution législative si ce concept reste lettre morte.

Modifications de la Loi sur l'impôt sur le revenu

Le Commissaire à la protection de la vie privée s'est également penché sur les modifications à apporter à la *Loi de l'impôt sur le revenu* et la *Loi sur la taxe d'accise* (projets de loi C-92 et C-132). Une fois adoptées, les modifications autoriseraient tout représentant de Revenu Canada l'impôt à utiliser les

l'élaboration d'un cadre de travail sur les principes de protection de la vie privée pour l'industrie des télécommunications. Ces principes ont surtout découlé de deux événements importants.

En premier lieu, le nouveau projet de loi C-62 sur les télécommunications, présenté en février 1992, décrivait ainsi l'un des huit objectifs stratégiques du gouvernement :

«...satisfaire les exigences économiques et sociales—notamment quant à la protection de la vie privée—des usagers des services de télécommunication.»

Le deuxième était la décision rendue par le CRTC concernant l'affichage téléphonique. Cette décision, qui infirmait un précédent jugement, mettait terme à ce qui est peut-être la question la plus controversée suscitée par l'introduction de services de gestion des appels par les compagnies de téléphone. En fin de compte, le CRTC a exigé que toutes les compagnies relevant de sa compétence offrent sans frais un service de blocage aux abonnés qui désirent éviter l'affichage de leur numéro.

L'affichage et le téléphone cellulaire sont deux exemples qui illustrent bien les côtés inattendus du progrès technologique. Dans les deux cas, la nouvelle technologie offre des commodités et des avantages importants; toutefois, sans certaines dispositions particulières, cela peut comporter un risque éventuel important pour la vie privée. Si le CRTC avait pu s'appuyer sur des principes sur la protection de la vie privée, il aurait pu prévoir les problèmes posés par les services de gestion des appels et les traiter au cours de sa première vérification. Cela aurait évité bien des ennuis, sans compter la nécessité de revoir, puis d'annuler, sa première décision.

Le ministre a adopté une approche volontaire pour la mise en œuvre de ces principes. Cette approche comporte des avantages

Ces modifications n'interdisent pas les balayeurs cellulaires et ne rendent pas illégale l'écoute indiscrète des appels faits par téléphone cellulaire, mais elles protègent dans une certaine mesure les conversations privées comme elle le fait déjà pour les conversations faites par le téléphone ordinaire.

Le Commissaire à la protection de la vie privée voudrait bien s'octroyer une partie du crédit pour avoir catalysé le processus législatif, mais il y a fort à parier que l'interception de l'appel Wilhelm-Tremblay au cours des négociations constitutionnelles (et la couverture médiatique ultérieure) a accompli davantage à cet égard en obligeant le législateur à se pencher sur le problème. Certains soutiendront que ces mesures ne sont pas assez sévères parce qu'elles n'interdisent pas, comme on le fait aux États-Unis, les balayeurs. Le Commissaire préférerait peut-être l'approche américaine—qui dénonce clairement l'interception en soi, —mais il est satisfait de toute mesure législative visant à mieux protéger la vie privée des Canadiens.

Principes de protection des télécommunications

Le deuxième développement important dans le domaine des télécommunications cette année résulte en partie d'un point abordé dans le dernier rapport annuel qui traitait de l'impact des progrès technologiques et de ce qui semblait être la futilité d'essayer de trouver des solutions techniques à chaque nouveauté technique. Le Commissariat avait entrepris d'énoncer de grands principes de protection de la vie privée et avait recommandé cette approche—empruntée à l'État de New York—au ministère des Communications en décembre 1991 et au Comité sénatorial sur le transport et les communications en juin 1992.

L'engagement pris par le ministre des Communications, ainsi que les ressources et les compétences de son ministère, ont abouti à

Le thème des télécommunications et de la vie privée revient constamment dans ces pages depuis plusieurs années. Une fois de plus cette année, nous avons des développements importants à signaler—de nouvelles dispositions législatives améliorant la confidentialité des communications faites par téléphone cellulaire et la publication par le ministère des Communications d'un ensemble de principes de protection de la vie privée dans les télécommunications. Deux autres projets ont reçu un accueil mitigé : la réglementation des institutions financières en matière de protection des renseignements personnels, et des modifications à la *Loi sur l'impôt*.

La protection des appels faits par téléphone cellulaire

Dans son rapport annuel de 1990-1991, le Commissaire signalait aux Canadiens la menace croissante à la vie privée que pose l'interception des appels faits par téléphone cellulaire. Deux cas fortement médiatisés—le premier concernant un ministre de la Colombie-Britannique qui a démissionné après qu'un journal ait publié des extraits d'appels effectués de sa voiture, le second relié au fait que des communications cellulaires auraient été interceptées au cours de la conférence du lac Meech—illustrent bien le problème.

Le Commissaire a incité le Parlement à agir rapidement afin de protéger la vie privée des usagers du téléphone cellulaire. Nous avons de bonnes nouvelles à annoncer. En décembre dernier, le gouvernement a déposé un projet de loi (C-109), modifiant le *Code criminel* et la *Loi sur les radiocommunications* afin de rendre illégale l'interception à mauvais escient de conversations privées faites par téléphone cellulaire et imposant des réparations civiles et des peines au criminel. Les modifications du *Code criminel* élargissent également la définition de ce qui constitue une communication privée pour y inclure les communications radiophoniques chiffrées.

pensionnés fédéraux. Les incidences de cette banque de données unique sont nombreuses : la liaison et la fusion des données, leur circulation entre les ministères, le besoin d'établir des mesures de sécurité et de restreindre l'accès aux personnes qui ont besoin des renseignements. Le défi sera de faire en sorte que ce système ne devienne pas un profil unique et global du gouvernement.

Le Commissariat examinera également le nouveau projet de rémunération de la Fonction publique, qui consiste en une base de données, unique et énorme, contenant les renseignements sur la paye et les avantages sociaux de tous les employés et

Système de rémunération de la Fonction publique

Le comité se penchera sur les résultats du projet et ses incidences (dont celles liées à la vie privée) et son rapport devrait paraître vers la fin de 1995.

Les mesures de sécurité protégeant les renseignements personnels doivent égaier celles offertes dans les locaux du gouvernement. Le degré de sécurité dépendra de la nature délicate des renseignements personnels et de la protection offerte par chaque agence gouvernementale. Il est évident que certains organismes permettront à leurs employés de travailler à distance avec des renseignements personnels, alors que d'autres l'interdiront.

Bien que le télé-travail puisse être bénéfique, le gouvernement a également reconnu qu'il comportait des incidences au niveau de la vie privée. Comment le gouvernement protégera-t-il les renseignements personnels des clients (et des employés) lorsque ces renseignements seront sortis de ses bureaux? Et comment assurera-t-il que le fait de travailler à la maison ne compromet pas la vie familiale de l'employé?

Le gouvernement a reconnu que la technologie de l'information pouvait nous aider à composer avec des questions sociales plus vastes comme le fait de permettre à un employé de mieux équilibrer les exigences de sa vie professionnelle et de sa vie privée, tout en réduisant la consommation d'énergie, la pollution et la congestion routière.

permettant à certains employés fédéraux de travailler à la maison et d'expédier électroniquement leur travail à leur employeur.

Le ministère des Communications (qui a déjà vécu une expérience décevante lors des premiers balbutiements de cette technologie en 1988) a entrepris plusieurs projets pilotes. Ces derniers visent notamment l'utilisation des cartes-mémoire pour contrôler l'inventaire de l'équipement de haute technologie coûteux à son Centre de recherche en communications et pour remplacer le contrôle des entrées et sorties des employés de l'Institut canadien de conservation. Le ministère des Communications prévoit également utiliser les cartes-mémoire comme « argent » électronique dans ses centres d'approvisionnement. Chaque carte contiendra un certain montant duquel sera débité chaque achat et chaque transaction sera enregistrée électroniquement.

Le ministère des Communications envisage également de consigner sur de telles cartes les mots de passe des employés donnant accès à divers systèmes informatiques. L'employé devra seulement se rappeler son numéro d'identification personnel qui lui donnera accès à ses divers mots de passe. Ces derniers seront chiffrés dans la mémoire de la carte afin d'en assurer la protection.

De telles cartes permettront de valider l'identité, la situation d'emploi et la cote sécuritaire d'un employé. On peut ainsi prévoir que le gouvernement fédéral se servira probablement de cette technologie pour créer une nouvelle carte d'emploi. Le défi sera d'assurer qu'elle ne devienne un outil de pistage. Cependant, le Commissariat est convaincu que le gouvernement saura concevoir des normes et des lignes directrices qui exploiteront la technologie, amélioreront la mise en œuvre de programmes et permettront de respecter la vie privée des personnes.

Travail à distance

Le groupe des cartes-mémoire n'est qu'un des divers comités au sein desquels siège le personnel du Commissariat. Le Comité qui se penchera sur le projet du travail à distance (télé-travail) en est un autre. Il évaluera les résultats d'un projet-pilote de trois ans

capable de contrôler et d'administrer ses programmes). Le gouvernement doit résister à la tentation de recourir à ces technologies pour surveiller ses citoyens de façon ouverte ou secrète.

Respect : Tous les intermédiaires doivent respecter les principes d'éthique ou les lois régissant la protection de la vie privée—tous les participants doivent connaître et respecter ces principes.

Responsabilité : Les personnes qui font la saisie des données doivent faire preuve d'un haut sens des responsabilités afin d'assurer la fiabilité du système.

Cette liste de contrôle peut paraître exigeante puisqu'elle pourrait imposer des démarches supplémentaires. Cependant, le principe de la protection de la vie privée peut être incorporé à la scène technologique de façon à garantir aux contribuables un service gouvernemental amélioré et une protection accrue de la vie privée.

Autres travaux en cours—cartes-mémoire

La liste de contrôle qui précède est tirée en grande partie du document intitulé *Cadre de travail des cartes-mémoire et vie privée* produit par le Commissariat dans le cadre de sa participation au sein du groupe de travail fédéral chargé de la mise en œuvre de cette nouvelle technologie. Ce document énonce un cadre d'éthique pour l'utilisation des cartes-mémoire, ainsi que des normes et des lignes directrices qui permettront d'incorporer la protection de la vie privée à la conception des applications faisant appel aux cartes-mémoire.

Le groupe de travail tente d'en cerner les applications possibles et de suggérer un cadre de travail opérationnel régissant l'utilisation de ces cartes.

Consentement averti : La personne doit être clairement informée de toutes les utilisations et les divulgations des renseignements traités la concernant et y consentir. Elle devrait également être autorisée à retirer son consentement sans préjudice.

Mesures de sécurité : Des mesures de sécurité doivent être mises en place afin d'éviter la mauvaise utilisation ou l'accès accidentel aux données personnelles. En d'autres termes, toute opération électronique doit être validée par l'utilisation d'un numéro d'identification personnel et protégée par des mécanismes de sécurité internes.

Couplage : Les systèmes que partagent plusieurs utilisateurs devraient être cloisonnés afin d'éviter toute fusion ou migration de renseignements personnels durant une opération. Toute opération impliquant l'ordinateur central doit également être protégée.

Accès : La personne doit avoir le droit d'accéder aux renseignements la concernant qui résultent d'une opération, et de corriger ces derniers au besoin.

Non-discrimination : Les nouvelles technologies ne doivent pas restreindre les services que le gouvernement offre à un client et les services offerts électroniquement doivent respecter l'universalité des programmes gouvernementaux. (Toutefois, il est évident que, même lorsque la participation est volontaire, les participants peuvent profiter d'avantages tels un service plus rapide ou un service après les heures d'affaires régulières).

Bienfaisance : Le gouvernement doit reconnaître et affirmer que les nouvelles technologies sont des outils qui lui permettront d'offrir des services et non d'exercer un contrôle sur les renseignements de ses clients. (Bien entendu, il y a des exceptions en ce sens que le gouvernement doit être

La question intéresse particulièrement le Commissariat, le Conseil du Trésor a donc invité le Commissaire à participer à ce projet à titre de conseiller sur la façon de protéger les renseignements personnels affectés par la mise en place de nouveaux services électroniques et systèmes de communication.

Cette invitation, acceptée avec plaisir, reconnaît de ce fait la place légitime de la vie privée dans le débat. Une protection raisonnable de la vie privée n'est pas incompatible avec l'évolution technologique; il s'agit simplement d'arriver à faire converger les disciplines qui intégreront des valeurs humaines à la conception et la mise en œuvre de nouveaux systèmes.

Le Commissariat espère aussi établir, avec des hauts fonctionnaires, un groupe de travail interministériel sur la vie privée et la technologie.

Dans un premier temps, le Commissaire a proposé une «liste de contrôle de la vie privée» dont se serviraient les hauts fonctionnaires à l'étape de la conception. Alors que se poursuit l'élaboration d'un «cadre de travail», cette liste permettrait d'assurer le respect de la vie privée des clients et des employés.

Liste de contrôle de la vie privée

Honnêteté et transparence : La personne doit être pleinement informée de ses droits face aux nouvelles technologies. Avant de lancer un nouveau système, le gouvernement doit aviser le public de son développement, de ses objectifs et de sa portée, du type de renseignements qui seront recueillis et utilisés et des personnes qui seront touchées. Toute personne doit aussi clairement savoir qu'elle a le droit de refuser de participer, de connaître la nature des renseignements visés par le processus technologique et les situations susceptibles de découler de l'utilisation de la technologie.

La prestation électronique des services

Au cours de la prochaine décennie, tous les gouvernements devront relever le défi d'être plus accessibles aux contribuables, de leur offrir de l'information, des services et des prestations directement, et ce en s'appuyant sur des ressources qui ne cessent de diminuer. La stratégie du gouvernement fédéral est donc d'améliorer ses services par l'utilisation innovatrice de technologies interactives.

En raison de la gamme de programmes et de services qu'offre le gouvernement, ces questions sont complexes et les coûts en investissements, énormes. De plus, les nouveaux progrès technologiques peuvent compromettre le contrôle individuel des renseignements personnels et la protection qu'offrent les lois portant sur la vie privée.

Le gouvernement fédéral a reconnu que, la technologie et les technologues avaient jusqu'ici isolé l'impulsion de la gestion des renseignements personnels. Il n'empêche cependant que la situation est sur le point d'évoluer. Le gouvernement admet maintenant que la technologie ne nous offre que des choix et que les valeurs humaines—y compris le respect de la vie privée—doivent entrer en ligne de compte durant le développement et la mise en œuvre de nouveaux systèmes d'information.

Tout d'abord, le gouvernement a mis sur pied un secrétariat des nouveaux services électroniques. Ce dernier, qui relève du Conseil du Trésor, a été chargé d'élaborer une perspective et un cadre de travail concertés sur l'introduction de nouveaux services électroniques. Le secrétariat aidera les ministères à se servir de la technologie comme principal moyen de renouvellement de leurs services, à déterminer lequel de ces services peuvent être fournis électroniquement et à les conseiller sur la meilleure façon de mettre en œuvre la technologie.

question est plutôt de savoir si les changements continueront d'être régis uniquement par les possibilités de la technologie, sans tenir compte de valeurs traditionnelles et fortement ancrées tel le respect de l'autonomie et de la vie privée des personnes.

De la poudre à canon à la fission nucléaire, les innovations techniques pourront servir autant à des fins bénéfiques qu'à des fins maléfiques. Les ordinateurs ne font pas exception. Encore une fois, le choix nous appartient. Mais le temps presse—les dix prochaines années pourraient sceller la question à jamais.

d'inscrire ces principes dans des codes ou des lois; ils doivent être disposés à établir des moyens leur permettant d'en assurer le respect.

Tous les gouvernements doivent reconnaître que les droits à la vie privée s'appliquent tant au secteur privé qu'au secteur public. Lorsque de tels droits n'existent pas, il appartient au gouvernement d'y suppléer.

La population canadienne a le droit d'être dûment informée des incidences possibles de la technologie sur sa vie—quelle information est requise, à quoi elle servira et comment en sera réglementé l'usage.

Un engagement de ce genre passe nécessairement par une bien meilleure éducation du public. Il exige également des efforts fédéraux-provinciaux concertés afin de réunir les spécialistes capables de comprendre et d'expliquer les incidences de la technologie sur la protection de la vie privée. L'établissement d'un organisme semblable au U.S. Office of Technology Assessment constituerait un bon point de départ, en aidant les décisionnaires à prévoir les conséquences des changements technologiques et à examiner comment la technologie influe sur l'existence des personnes.

L'objectif, à présent, devrait être de renforcer et d'élargir la protection. Bien entendu, lorsque plus d'une compétence est touchée, l'une d'entre elles doit ouvrir la marche. À cet égard, il semble évident que le gouvernement du Canada est le mieux placé pour montrer la voie. Le Commissaire recommande que le Parlement prenne des mesures afin de mettre au point un plan national visant la réalisation des objectifs énoncés dans les principes proposés.

Il faut se rappeler que la question n'est pas de savoir si la technologie continuera de changer nos vies. Cela est acquis. La

De façon générale, cela signifie que les renseignements personnels doivent être recueillis uniquement lorsqu'ils sont vraiment nécessaires, employés aux seules fins établies au préalable, divulgués dans des circonstances très clairement définies et accessibles au principal intéressé, lequel doit également avoir le droit de demander que des corrections soient apportées. Les gouvernements ne doivent pas se contenter

Tous les gouvernements doivent reconnaître que la population canadienne a droit à la protection de ses renseignements personnels tel qu'il est énoncé dans des documents comme les *Lignes directrices régissant la protection de la vie privée de l'OCDE* et la *Loi sur la protection des renseignements personnels* du gouvernement fédéral.

La population canadienne a droit au respect de sa vie privée et ce, quels que soient la compétence gouvernementale, le secteur industriel ou la technologie en cause. Pendant le récent débat constitutionnel, le Commissaire a fermement plaidé en faveur de l'enchaînement d'un droit explicite à la vie privée dans la *Charte*. Cependant, ce sujet ne figurait pas au nombre des priorités. Quoiqu'il en soit, il est impératif d'élaborer un ensemble de principes pour garantir ces droits, comme suit :

révolution informatique.

problème, visant à concilier la protection de la vie privée et la

une démarche plus énergique et mieux coordonnée dans ce

domaines et nous y reviendrons. Mais le temps est venu d'adopter des initiatives qui méritent une mention honorable dans plusieurs

annuel que celui-ci font état de progrès encourageants : il y a eu les sérieux efforts en cours. Au contraire, tant le dernier rapport

Les observations ci-dessus ne discréditent ni ne diminuent en rien

la vie privée, soit un ensemble de principes qui serviront de critères pour l'évaluation des nouveaux produits et services.

téléphonique connaîtra (comme l'indiquera le relevé de compte) l'emplacement des deux interlocuteurs ainsi que le moment de l'appel. Ces dossiers seront-ils mis à la disposition du gouvernement? De la police? Seront-ils vendus à des fins de marketing?

Braver les conséquences

Doit-on continuer de faire valoir l'impérieuse nécessité d'un meilleur contrôle du commerce de l'information? Dans la course à l'information, il y a très peu de place pour des efforts visant à garantir un respect raisonnable des droits des personnes qui sont à la source des renseignements constituant la matière première de ce secteur. Dix ans après que le premier Commissaire à la protection de la vie privée ait dévoilé cette «menace», le fossé entre le problème et la solution n'a cessé de s'élargir.

Il devient de plus en plus lassant d'entendre clamer par des personnes intéressées à préserver la libre circulation des données à quel point il est «difficile» de protéger la vie privée quand on les soupçonne de penser plutôt au mot «incommodant».

Comment ne pas remarquer combien les solutions sont faciles à trouver lorsque des cas particuliers sont étalés au grand jour. Le récent exemple de l'interception des conversations faites par téléphone cellulaire en est la preuve. Du moment que des divulgations politiques de nature délicate ont exposé la vulnérabilité de ces dispositifs à la vue des politiciens et du public, l'appareil législatif a réagi de façon remarquablement rapide pour proposer une solution.

La preuve a été bel et bien faite récemment qu'il existe des solutions. Il reste maintenant à trouver la volonté de s'attaquer à la question dans son ensemble. Ces dix dernières années nous ont enseigné que le rythme de l'évolution technologique est trop rapide pour permettre l'improvisation d'une solution pour chaque nouvel outil qui apparaît. Il est impossible de prévoir où nous

L'utilité de ces dispositifs ne peut cependant occulter les problèmes de protection de la vie privée qui en découlent. Non seulement existe-t-il des risques pour les appels en soi—il s'agit de communications sans fil, après tout—mais plus insidieux encore sont les risques sur le plan de la surveillance. À peine avons-nous en effet composé le numéro que le service

Le texte et l'image.
nouveaux dispositifs pourront indifféremment traiter la voix, le son, parviendront à leurs destinataires, où qu'ils se trouvent. Les des émetteurs radioélectriques, des satellites et des ordinateurs et lieux, mais à des personnes. Les appels seront acheminés par pour les Canadiens. Des numéros seront affectés, non plus à des Ces derniers sont appelés à redéfinir l'utilisation du téléphone nouveau véhicule de communication—les réseaux personnels. Les cinq prochaines années verront aussi l'apparition d'un

comme les radiographies et les électrocardiogrammes.
des dossiers médicaux informatisés, mais également des images cheveu non seulement les mots des messages électroniques et communications, transportant sur des fibres aussi minces qu'un La grande autoroute optique viendra révolutionner les

routeurs durant notre siècle.
marchandises au siècle dernier, et que l'ont fait les réseaux transcontinental a transformé le flux des personnes et des le flux de l'information de la même façon que le réseau ferroviaire électroniques sera 2 000 fois plus élevée. Ce réseau transformera ans, la quantité de données acheminées par des réseaux an dans ce projet pendant les cinq prochaines années. Dans cinq part, le gouvernement fédéral injectera des millions de dollars par et public et les citoyens de tout le pays d'ici l'an 2000. Pour sa haute vitesse dont les fibres optiques relieront les secteurs privé l'enseignement (CANARIE), reposera sur un réseau numérique à pour l'avancement de la recherche, de l'industrie et de personnels de communication. Le premier, le Réseau canadien réseaux d'information nationaux et les nouveaux appareils

«...il est banal de dire que la vie privée est menacée comme elle ne l'a jamais été dans l'histoire...La convergence de techniques nouvelles et de revendications toujours plus insistantes de l'État en vue de savoir ou d'être efficace ou les deux a modifié la nature quantitative et qualitative du problème.»

Si la menace était déjà si bien comprise et visualisée il y a dix ans, que penser de la situation d'aujourd'hui? Exception faite de certains cas, c'est bien pire encore. Chacun est conscient de l'essor incroyable du marketing direct—l'avalanche de publicité postale et les appels de sollicitation en soirée, par exemple. Tout indésirable que ce genre de sollicitation soit (et sans grave conséquence, ajouteraient certains), il n'en exige pas moins l'accès à des profils très détaillés de clients éventuels. Pourtant, bien peu d'entre nous savons ce que renferment ces profils, d'où provient l'information sur laquelle ils sont fondés, qui les détient, à quel point ils sont exacts ou adéquatément protégés et, pis encore, à qui ils pourraient être vendus.

En réalité, ces dix ans de progrès technologiques ont transformé la valeur inhérente des renseignements personnels. Chaque parcelle d'information à notre sujet intéresse quelqu'un, des données insignifiantes en apparence comme notre nom ou notre âge, à des renseignements sur notre mode de vie comme nos habitudes de consommation ou nos préférences cinématographiques jusqu'à des données médicales précises comme nos traits génétiques. La technologie nous a donné les outils nécessaires pour acheter, manipuler, reconstituer ou vendre les détails de la vie des autres afin d'en tirer profit. Les Canadiens n'échappent pas à l'oeil scrutateur de toute cette technologie électronique; ils laissent une piste visible—des détails sur leurs renseignements personnels et leurs opérations—qu'ils ne peuvent contrôler.

Examinons les incidences sur la vie privée de seulement deux de ces innovations technologiques : les nouveaux et puissants

Il y a dix ans, le premier rapport du Commissaire à la protection de la vie privée faisait observer :

Laisser une piste visible

Qui pourrait se sentir tranquille après la lecture de tels cas ?

- un homme qui vérifiait l'exactitude de son dossier de crédit a découvert que plusieurs demandes avaient été faites à son sujet par un avocat d'une province où il n'a aucun lien d'affaires ou personnel. Cet homme n'a aucun recours juridique étant donné qu'il n'existe pas de loi nationale en matière d'information financière ni de mesures de protection des renseignements personnels dans le secteur privé.
- une banque à charte a divulgué les numéros de cartes, les noms, les adresses et d'autres données personnelles sur ses clients à des services d'étude du marché pour vérifier la demande de nouveaux produits;
- huit employés d'un service d'information financière ont faussement allégué être à l'emploi de Revenu Canada afin de retracer des clients qui devaient de l'argent à un service provincial de services publics;
- une entreprise chargée de détruire des dossiers médicaux de nature délicate les a vendus à une société de productions télévisées qui s'en est servie comme accessoires lors de tournages;
- une chaîne d'alimentation a entrepris d'émettre des « cartes de service » donnant droit à des rabais à ses clients, mais elle a omis de les informer que leurs habitudes de consommation seraient fichées et vendues à des entreprises de marketing direct;

Ceux qui ont pour tâche d'étudier la question savent très bien combien les Canadiens ont raison sur ce point.

La population canadienne est au fait de certains cas d'indiscrétions rapportées à grand fracas par les médias et mettant en cause des conversations par téléphone cellulaire. Mais il y a fort à parier que ce n'est là que menu fretin comparativement aux renseignements personnels qui circulent entre les bases de données informatisées et auxquelles ont accès des personnes dont le droit à cette information est, au mieux, discutable.

Aux États-Unis, grâce aux nombreuses enquêtes effectuées par le Congrès et la grande persistance des milieux médiatiques, une somme considérable de connaissances sur la portée et la nature des échanges de renseignements entre les bases de données informatisées a été rassemblée. Et ce ne sont pas les histoires d'horreur qui manquent. Par exemple, dans l'un de ses plus récents ouvrages, « Privacy for Sale », Jeffrey Rothfeder (qui n'est pas un spécialiste de l'informatique) raconte comme il lui a été facile d'obtenir accès aux dossiers de crédit sur l'ancien vice-président des États-Unis, Dan Quayle, et le présentateur de nouvelles, Dan Rather.

L'auteur raconte aussi comment, par suite d'une erreur de saisie, la totalité des résidents d'une petite municipalité de la Nouvelle-Angleterre avaient été portés sur la liste des fraudeurs fiscaux par un service d'information financière. Aucun des 1 500 résidents n'étaient au courant de cette tâche accablante et inexacte sur leur dossier de crédit jusqu'à ce que l'un d'entre eux, un médecin en vue (peu habitué, sans doute, à se voir refuser du crédit), ne creuse la question.

Compte tenu des similitudes entre les pratiques commerciales canadiennes et américaines, il y a lieu de présumer que ce genre de choses pourrait très bien survenir au Canada. Voici, pour n'en mentionner que quelques-uns, des exemples récents puisés dans les médias :

d'envergure nationale sur les attitudes du public à l'égard des questions de protection de la vie privée vient jeter un éclairage utile sur le sujet. L'étude apporte la première preuve statistique tangible que la population canadienne est consciente de cette question—une preuve irréfutable, s'il en fallait une, que la protection de la vie privée n'est pas une préoccupation élitiste ou une question d'importance secondaire. Le fait que 52 p. 100 de la population se soient dits «extrêmement préoccupés» par la situation relativement à la protection de la vie privée devrait satisfaire les plus sceptiques des législateurs ou des autorités de réglementation. Il existe un fort consensus, au sein du public, pour en faire une plus grande priorité politique.

L'enquête, parrainée et financée par un groupement d'organisations des secteurs privé et public (y compris le Commissariat), a aussi révélé que les Canadiens savent ce dont ils ont besoin pour protéger leur vie privée dans une société axée sur l'information. L'immense majorité dit vouloir conserver une forme de contrôle sur la collecte des renseignements à leur sujet, être prévenue de la collecte de telles données, connaître les responsables et les objectifs de la collecte, et avoir le droit d'accepter ou de refuser toute opération exigeant l'emploi de ces renseignements personnels. Bref, la population réclame des choses qui vont au cœur même des pratiques équitables en matière d'information et qui font bien souvent défaut, aujourd'hui, dans la circulation des renseignements personnels.

Notre population a donc saisi la problématique de la protection de la vie privée en cette ère de l'information : le contrôle personnel des renseignements qui sont détenus ou accessibles par d'autres à leur sujet. L'enquête révèle un malaise très répandu—61 p. 100 sont **fortement** d'accord avec l'énoncé voulant que les consommateurs aient perdu tout contrôle sur la circulation et l'utilisation de leurs renseignements personnels par les entreprises. En outre, 60 p. 100 conviennent qu'ils jouissent maintenant d'une intimité moindre, en général, qu'il y a 10 ans.

commerciale dans un environnement où la concurrence est de plus en plus vive.

À coup sûr, les menaces qui pèsent sur la protection des renseignements personnels ne représentent qu'un aspect du problème global de protection de la vie privée. La montée des atteintes à la vie privée et l'accroissement de la surveillance physique complètent le dilemme. Ces atteintes débordent sans doute du cadre général du présent rapport sur la protection des renseignements personnels, mais elles n'en constituent pas moins un élément crucial du phénomène de l'ingérence.

À quand l'apparition de caméras aux coins des grandes artères de nos villes pour mieux prévenir le crime? Au nom de la lutte contre le crime, les Canadiens pourraient être soumis à la surveillance de l'État dans leurs faits et gestes les plus légitimes? Orwell a peut-être vu juste.

L'utilisation croissante de la technologie dans la surveillance des employés ne présage rien de bon. Chaque nouvelle forme de surveillance nous déshumanise davantage, au point où nous devenons de plus en plus ravalés au rang d'automates et destinés, en cas d'imperfections ou de comportements anormaux, à aller grossir la pile des modèles défectueux ou à faire l'objet de «mesures correctives».

Certains spécialistes soutiennent que la partie est déjà perdue puisque notre vie est déjà mise à nu par la technologie. Selon eux, les Canadiens devraient reléguer la notion du contrôle individuel à l'histoire, arrêter de s'en faire et apprendre à vivre au sein d'une merveilleuse et libre circulation de l'information.

La vie privée exposée

Heureusement, durant les dix dernières années, le public a pris de plus en plus conscience de l'incidence de la technologie sur la vie privée. La publication, au printemps de 1993, de la première étude

Extase technologique

Loin de lui l'idée de se complaire dans l'autosatisfaction, toutefois, car, de plus en plus, force lui est d'admettre qu'il en sait juste assez pour se rendre compte qu'il en connaît au fond bien peu. Le Commissariat consacre une bonne partie de son temps à courir au plus pressé. Et quant au vaste monde au-delà du gouvernement fédéral et de la portée de la Loi sur la protection des renseignements personnels, il est peut-être trop tôt pour fêter. Pris dans ce contexte plus large, plusieurs développements dans la dernière décennie ont effectivement durement touché la protection de la vie privée. Ce sont :

- la progression fulgurante des technologies de l'information, des gros ordinateurs aux carnets électroniques, en passant par les micro-ordinateurs. Chaque étape a donné naissance à des outils sans cesse plus petits, plus mobiles, plus puissants et plus faciles à relier entre eux en réseaux mondiaux, ainsi qu'à des logiciels dotés de possibilités de plus en plus grandes;

- l'acceptation aveugle de la technologie dans les sociétés occidentales, allant même jusqu'à négliger d'examiner les incidences sur les droits individuels. Nous évoluons dans ce qui a été qualifié « d'extase technologique ». La technologie dicte les droits individuels alors que ce devrait être l'inverse, et la réaction des secteurs privés et public a été sporadique, hésitante et d'une efficacité toute marginale;

- l'évolution rapide de la biotechnologie qui, d'un outil conçu pour améliorer la santé humaine, est devenue une arme commerciale et politique redoutable offrant d'inquiétantes possibilités de surveillance et de contrôle de la société;
- la transformation en valeur marchande de l'information, qui est devenue un bien commercial menant à la compétitivité

L'un des nouveaux systèmes proposés est un réseau interactif de kiosques d'information gouvernementaux (les « Centres-Info ») grâce auquel les clients pourraient obtenir de l'information sur les services du gouvernement, prendre connaissance des offres d'emploi, s'inscrire à divers programmes et transmettre leur changement d'adresse aux ministères participants. Une fois sur pied, le réseau pourrait être enrichi de façon considérable jusqu'à devenir un centre d'accès unique à la totalité des services du gouvernement fédéral.

Ces nouveaux systèmes électroniques suscitent des modifications profondes dans le traitement de l'information par le gouvernement, dont trois sont alarmantes. La première est la nécessité d'utiliser une carte d'identité pour recevoir les services, ce qui sous-entend l'emploi d'un numéro personnel d'identification, probablement une photographie et, fort peut-être, des empreintes digitales ou quelque autre mode d'identification biométrique.

La deuxième a trait à la participation vraisemblable du secteur privé à tout échange électronique de renseignements personnels, secteur qui n'est actuellement assujéti à aucune loi régissant la protection de la vie privée.

La dernière découle du fait que le coût de développement et de prestation de ces nouveaux services pourrait forcer le gouvernement à consolider ses programmes dans l'ensemble des ministères—et même, peut-être, à l'échelon des champs de compétence fédéraux et provinciaux. Cela pourrait sonner le glas des bases de données distinctes ce qui, de nouveau, fait surgir le spectre du dossier—ou du profil—unique et le personnage inquiétant de Grand Frère.

Le Commissaire à la protection de la vie privée a donc un programme bien chargé.

Le Commissariat peut affirmer avoir, jusqu'à un certain point, contribué à stimuler le débat public au sujet du couplage des données, du contrôle du numéro d'assurance sociale, des incidences de la biotechnologie sur la protection de la vie privée, des principes de protection de la vie privée dans les services de télécommunications, des mesures pour éviter l'écoute subreptice des conversations faites par téléphone cellulaire, des règlements en matière de protection des renseignements personnels dans le secteur financier et de l'enchâssement des droits en matière de protection de la vie privée dans la *Charte*.

Nombre de ces initiatives témoignent de façon frappante de l'évolution du rôle de ce petit Commissariat. Mandaté (et subventionné) uniquement pour faire enquête sur les plaintes déposées contre quelque 160 institutions fédérales, le Commissaire est pressé par les parlementaires, le grand public et les médias de répondre à leurs questions en matière de protection de la vie privée, de donner son avis sur les incidences que peuvent avoir sur la protection de la vie privée les nouveaux programmes et les nouvelles lois, de comparaître devant des comités et de s'exprimer sur des questions qui débordent de son étroit mandat. Refuser l'exposerait à manquer d'à-propos. Accéder compromet sa solvabilité. L'ombudsman du gouvernement en matière de protection de la vie privée s'efforce de répondre aux demandes, mais sa situation budgétaire a atteint un point critique.

Les restrictions financières actuelles ont toutefois des répercussions beaucoup plus vastes sur le plan de la protection de la vie privée. Mis au défi de rationaliser les programmes, d'améliorer les services et de comprimer les coûts, le gouvernement recherche résolument des moyens d'informatiser le maximum d'activités. Le dépôt direct des chèques de prestations n'est qu'un début. Le gouvernement utilise déjà l'échange de données informatisées (EDI) pour percevoir la TPS et l'impôt sur le revenu des particuliers, pour recueillir des renseignements sur les immigrants et les réfugiés et pour percevoir les droits de douane aux frontières.

La publication du présent rapport coïncide avec le 10^e anniversaire de l'entrée en vigueur de la *Loi sur la protection des renseignements personnels* du gouvernement fédéral et de la création du Commissariat à la protection de la vie privée. À une telle occasion, il est tout naturel de se demander si cet avènement a été un bienfait.

La célébration de cet anniversaire est de bon augure puisque le sujet est toujours là pour célébrer. Et, assurément, la progéniture est des plus prometteuses. Néanmoins, il ne nous semble pas indiqué de sabler le champagne.

L'événement nous inspire plutôt une satisfaction contenue. Le Commissariat se réjouit d'avoir été utile aux Canadiens durant ces dix ans en les aidant à exercer leurs droits relatifs à la protection de leurs renseignements personnels dans leurs rapports avec le gouvernement du Canada. Nous avons achevé au-delà de 7 500 enquêtes, répondu à près de 25 000 demandes de renseignements réglées ainsi que d'importantes vérifications ayant touché le tiers environ des fonds de renseignements du gouvernement. Ce n'est pas négligeable pour un Commissariat dont l'effectif n'a jamais dépassé plus de trente-six personnes.

Les prédictions les plus sombres des sceptiques ne se sont pas concrétisées : la vigilance ne s'est pas relâchée, il n'y a pas eu de renonciation en masse aux principes d'une saine gestion des dossiers et les ministères ne se sont pas constamment retrouvés devant les tribunaux. Aucun ministère n'a encore été terrassé par le volume des demandes des citoyens souhaitant examiner leur dossier personnel (quoique la Défense nationale en ait souffert jusqu'à ce qu'elle modifie sa politique).

En réalité, la *Loi*, les plaintes et les vérifications ont incité de nombreuses institutions gouvernementales à mieux déterminer, organiser et affiner leurs systèmes de gestion de dossiers, ce qui constitue un grand avantage au moment où la presque totalité des organismes gouvernementaux se sont convertis à l'informatique.

54	Au Commissariat...
54	La Direction des plaintes
54	Performance des institutions
58	Communications au Commissaire
65	Demandes de renseignements
69	Cas particuliers
84	Tableaux
89	Au Commissariat...
89	Évaluation de l'observation
90	Enquêtes spéciales
92	Vérifications de conformité dans les institutions
96	Suivi
101	En l'an 1993—Où sont vos renseignements?
107	Gestion intégrée
109	Organigramme

Table des matières

Dix ans plus tard	1
Relever le défi de la technologie	
La prestation électronique des services	15
Liste de contrôle de la vie privée	16
Autres travaux en cours	18
Sur la colline parlementaire	
Protection des appels faits par téléphone cellulaire	22
Principes de protection des télécommunications	23
Modifications de la <i>Loi sur l'impôt sur le revenu</i>	25
La vie privée et les institutions financières	29
Dans la rue	
<i>La vie privée exposée</i> —sondage canadien sur la vie privée	31
Actualités juridiques	
Le CPVP et la Société canadienne des postes	34
Le NAS pour l'enregistrement de la naissance	35
Une patiente gagne accès à son dossier médical	36
...Dans les laboratoires	
Le dossier de la biotechnologie : quoi de neuf?	38
Ici et là...	
À l'échelon provincial	44
À l'étranger	46
Dans le secteur privé...	
Code modèle de l'Association canadienne de normalisation	51
Code de protection des renseignements personnels de l'Association canadienne du marketing direct	52

Voici en quoi consiste la mission du Commissaire à la protection de la vie privée.

- être un protecteur efficace des droits des citoyens qui mène, en temps opportun, des enquêtes approfondies afin que la population canadienne puisse jouir des droits que lui accorde la *Loi sur la protection des renseignements personnels*;
- protéger efficacement, au nom du Parlement, la vie privée et évaluer de façon professionnelle dans quelle mesure le gouvernement respecte les dispositions de la *Loi sur la protection des renseignements personnels*;
- conseiller le Parlement sur les questions liées à la protection de la vie privée, et lui fournir, grâce aux activités de recherche et aux communications, les faits qui lui permettent de rendre des jugements avisés;
- être le principal centre national de ressources pour la recherche, l'éducation et l'information en matière de protection de la vie privée.

Le Commissaire à la protection de la vie privée est un ombudsman spécialisé—nommé par le Parlement et tenu de lui rendre compte,—qui surveille la façon dont le gouvernement fédéral recueille, utilise et communique les renseignements personnels de ses clients et de ses employés, et répond aux demandes des personnes souhaitant consulter leurs dossiers.

La Loi sur la protection des renseignements personnels donne au Commissaire de vastes pouvoirs pour enquêter sur les plaintes dont il est saisi, de lancer sa propre plainte et de vérifier si les quelque 160 organismes gouvernementaux assujettis à la *Loi* en respectent les dispositions. Il effectue aussi des activités de recherche de son propre chef ou à la demande du ministre de la Justice.


L'honorable John A. Fraser, c.p., c.r., député
Président
Chambre des communes
Ottawa

le 30 juin 1993

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Le rapport couvre la période allant du 1^{er} avril 1992 au 31 mars 1993. Veuillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée


Bruce Phillips

L'honorable Guy Charbonneau
Président
Sénat
Ottawa

le 30 juin 1993

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Le rapport couvre la période allant du 1^{er} avril 1992 au 31 mars 1993. Veuillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée

Bruce Phillips

Bruce Phillips

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-2410, 1-800-267-0441
Télec. (613) 995-1501
ATS (613) 992-9190

© Groupe Communication Canada
N° de cat. IP 30-1/1993
ISBN 0-662-59840-7

Cette publication est offerte sur cassette.

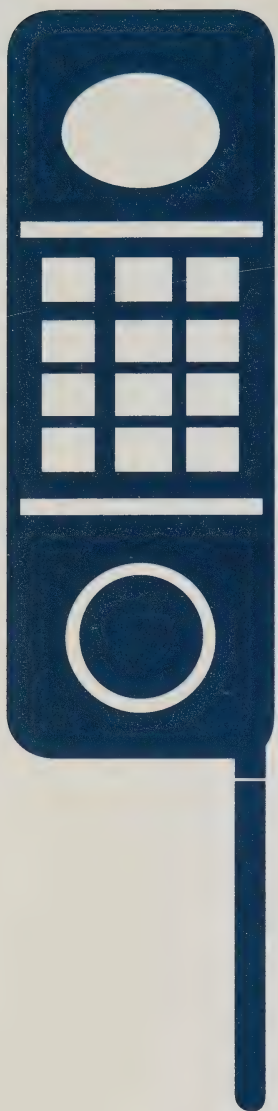
**Rapport annuel du
Commissaire à la protection
de la vie privée
1992-1993**





Commissaire à la
protection de la vie privée

Rapport annuel 1992 - 1993



For 1993/94 issue see:

CA7

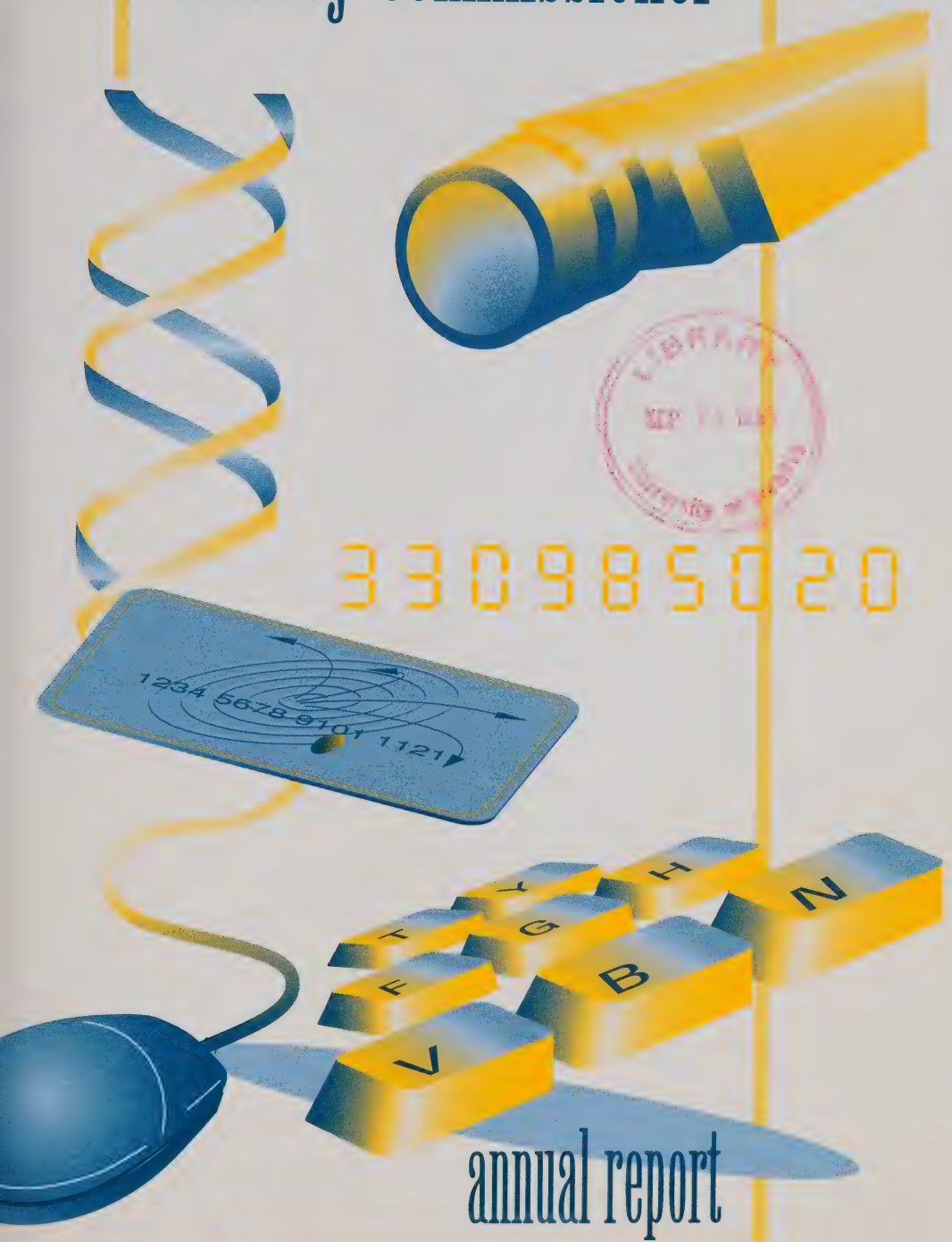
MM

-P65

#94-07304

CAI
PC
-A 57

Privacy Commissioner



330985020

annual report



1994 - 1995

Annual Report Privacy Commissioner 1994-95



The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 994-2410, 1-800-267-0441
Fax (613) 995-1501
TDD (613) 992-9190

© Canada Communications Group
Cat. No. IP 30-1/1995
ISBN 0-662-61956-0

This publication is available on audio cassette, computer diskette and on the Office's Internet home page at <http://info.ic.gc.ca/opengov/opc/privacy.html>



Privacy
Commissioner
of Canada

Commissaire
à la protection de
la vie privée du Canada

The Honourable Gildas L. Molgat
The Speaker
The Senate
Ottawa

July 1995

Dear Mr. Molgat:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1994 to March 31, 1995.

Yours sincerely,

A handwritten signature in dark ink, reading "Bruce Phillips". The signature is written in a cursive style with a large, looping "B" and a long, sweeping "P".

Bruce Phillips
Privacy Commissioner



Privacy
Commissioner
of Canada

Commissaire
à la protection de
la vie privée du Canada

The Honourable Gilbert Parent
The Speaker
The House of Commons
Ottawa

July 1995

Dear Mr. Parent:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1994 to March 31, 1995.

Yours sincerely,

A handwritten signature in cursive script that reads "Bruce Phillips".

Bruce Phillips
Privacy Commissioner

Gerard J. C. van Berkel

Gerry van Berkel died on January 5, 1995, barely six months after retiring as general counsel to the Privacy Commissioner, a position he held since the Office was created in 1983.

He was both an extraordinary human being and an unusual lawyer. The poet Marvell's words are apt: "He nothing common did or mean, upon that memorable scene". He had an expansive view of the law, seeing it as an instrument for human betterment, rather than a code of strictures for human regimentation. He was often heard to say that "the law should not stand in the way of helping people", and this attitude, animated by his common sense and compassion, made him an ideal counsel for an ombudsman's office.

Gerry van Berkel had been a government lawyer for three decades, having served as well in the Department of Labour and the Canadian Human Rights Commission. Wherever he went, he left behind a legion of friends and admirers. The staff of this Office were the particular beneficiaries of his mature wisdom, his wit and his patience; not to mention his good humoured tolerance of their gratuitous and unschooled legal opinions.

But they also knew him as a raconteur of note, chef extraordinaire, mean pop pianist, gifted cabinetmaker, but above all, devoted family man and loyal friend. All in all, a formidable work of the Creator in whom he had an abiding faith.

To him, in love and respect, this report is dedicated.

Mandate

The Privacy Commissioner is a specialist ombudsman appointed by and accountable to Parliament who monitors the federal government's collection, use and disclosure of its clients' and employees' personal information, and its handling of individuals' requests to see their records.

The *Privacy Act* gives the Commissioner broad powers to investigate individuals' complaints, to launch his own complaint, and to audit 110-odd federal agencies' compliance with the *Act*. He also conducts research on his own behalf or at the request of the minister of justice.

Mission

The Privacy Commissioner's mission is

- to be an effective ombudsman's office, providing thorough and timely complaint investigations to ensure Canadians enjoy the rights set out in the *Privacy Act*;
- to be an effective privacy guardian on Parliament's behalf, performing professional assessments of the quality of the government's adherence to the *Privacy Act*;
- to be Parliament's window on privacy issues, arming it with the facts needed to make informed judgements through research and communications;
- to be the primary national resource centre for research, education and information on privacy.

Highlights

- Federal government leadership needed now to protect Canadians' privacy in the private sector—starting with the banking, telecommunications and interprovincial transportation sectors where it has jurisdiction (page 6)
- Changes to the census to better protect Canadians' privacy—and an outstanding issue (page 33)
- End to random drug testing of Forces' members (page 16)
- How to devise an electronic privacy system—Public Key Infrastructure (page 8)
- Safeguards for the public's and employee's tax files during internal Revenue Canada investigations (page 22)
- Removal of gratuitous personal details from public bankruptcy files (page 70)
- Improved controls on disposal of surplus assets— computers, diskettes and file cabinets (page 60)
- 1307 complaint investigations and almost 10,000 inquiries handled; a record 1,783 new complaints (page 31)

Table of Contents

There is a tide...	1
Update: Privacy, Security and the Information Highway	8
From post box to E-mail to public key	
infrastructure—a primer	10
Update: A Model Privacy Code for the Private Sector	14
Update: Biomedical Privacy	16
The watch on drug testing	16
DNA testing in criminal investigations	18
A model genetic Privacy Act	20
Update: Safeguarding Tax Files	22
Update: The Privacy Patchwork	24
In the Courts	26
Privacy and Access of equal weight	26
Denied adjudicators' notes—case goes to court	27
Consulting the Commissioner— MPs' pensions	28
Investigating Complaints	31
The Cases	33
Inquiries	50
Monitoring Compliance	58
Disposing of surplus assets	60
Sharing personal information— agreements	
and "arrangements"	62
Notifying the Commissioner	67
Audits and Follow-ups	70
Consumer and Corporate Affairs, Immigration, Pacific	
and Atlantic Pilotage Authorities, Canada Council	70
Follow-ups	75
Office of the Chief Electoral Officer	76
Corporate Management	78
Organization Chart	80

**There is a tide in the affairs of men,
Which, taken at the flood, leads on to fortune;
Omitted, all the voyage of their life
Is bound in shallows and in miseries.**

—Julius Caesar, Act IV, Scene III

Right on, Mr. Shakespeare! Nowadays we're not so elegant of speech. Translated into 1995-ese, we'd probably say "Let's move it", or something even more blunt. But the meaning is the same: the time for action is now.

Events have moved swiftly in the past year. We are now at that critical point at which decisions must be made which either will "lead on to fortune" or to "shallows and miseries".

Those decisions in the main are in the hands of our governments, so this is a plea to them to meet this opportunity with courage and foresight, resisting along the way the inevitable pressure from special interests for weak-kneed half-measures. Timidity in defence of human rights is no virtue.

But first let's step back for a moment and scan the landscape across which we are travelling. Most people now are aware of the immensity of the changes which technology is working on society. Information technology in particular is throwing dazzling lights of knowledge across the worlds of commerce, academia, science, medicine and government, in fact every aspect of human life. But we must take care that the light does not blind us to our duty to ensure that we reap those benefits without sacrificing older values essential to the protection of human rights which are the foundation of civilized society.

Over centuries of evolution of Western thought, one constant has been the acceptance of the individual's right to defend that uniqueness by exercising some control over the ability of others to intrude or impose. The technology revolution is making a shambles of that right.

"Information" is not a single substance or entity. It is not just data. It is not a product or a commodity. Whether conveyed by voice, recording, printed word, picture, digitized code, sign language or sight, information is the expression of all that we know and are. Personal information expresses the substance of individual lives; in short, all the things which distinguish one human being from another, which certify the uniqueness of each individual.

"Privacy", in fact, is not a word adequate to describe the problem. In the technological context, some experts describe it as "the right to informational self-determination", or the right "to control what others know about you". These are good descriptions, but they only reflect a more profound underlying issue—the degree to which, in the new information age, we will respect each other as individual human beings.

Brave new words

Previous reports have attempted to alert Parliament and public to the lethal threat to the preservation of some reasonable degree of personal privacy posed by the indiscriminate or unthinking application of information technology. Now, it must be said, there has been a significant change in the level of public awareness. Poll after public opinion poll has demonstrated rising public uneasiness. Routinely they show 80 or 90 per cent of those interviewed are concerned about the assault on their privacy. They suspect, rightly, that much is going on which is not explained adequately to them, and that worse may be to come.

These polls frequently also show that such fears are coupled with a strong appetite for government action. The public knows the world is changing swiftly, and is anxious not to be left naked in an environment more threatening to personal autonomy than anything we have known before. From a state of general indifference, privacy protection has forced its way, if not onto centre stage, at least to reasonable prominence on the agenda of issues worthy of attention.

Doubtless this is less the result of any individual effort than the accumulation of evidence obvious to almost everyone—this is not simply an abstract philosophical problem but one that affects everyday life. Whatever the reason, we have attained the necessary pre-condition to effective action. However, we must not confuse recognition with

solutions. There is much talk but few results. But compared with a few years ago, even that is real progress.

One thing is abundantly clear. The next year or two will tell the tale, whether as a society we care enough about our personal autonomy and individuality to defend it against the clamant pressures of the economic bottom-line, or are content to see ourselves digitized into data subjection.

There is nervous optimism. Optimism because there is strong support in important quarters for enhanced privacy protection in the age of information technology. One such notable support is the committee work of the government's Advisory Council on the Information Highway (of which more later). The nervousness stems from the power of private interests to resist change, coupled with a prevailing climate which militates against government action in the commercial sphere. Even times such as these, however, offer no justification for failing to protect those defining values. Easy times and not-so-easy times come and go. Respect for human rights must remain the bedrock of society, immune alike to breeze of prosperity and blast of hardship.

The issue is clear: the preservation of a private life in the information age depends upon our retaining some control over what the world knows about us. This control has all but disappeared except in the limited areas where privacy laws exist; principally in the public sector. Only stronger legal defences can restore control.

There is now almost universal agreement with these two propositions. The Canadian private sector, which generally operates free of any legislated privacy rules (except in Quebec) now recognizes the rising tide of public concern. Many businesses have attempted to meet this concern by drafting their own privacy codes. And there's the rub. While conceding a problem, there is still much opposition to the idea of anything more than "voluntary" or "self-regulated" observance of privacy rights. That's to say, we know there's a traffic problem but please, no traffic cop.

Optional privacy rights?

Reluctantly, and by stages, this writer has come to the view that "voluntarism" is inadequate. The reasons are several. The first; collection of personal information, much of it without our knowledge or consent, is now a huge business and getting more huge all the time. As individuals, we have a right to exercise some control over this traffic, but all the jawboning of recent years has had little impact.

The second reason; technology is accelerating this process, and the longer it proceeds devoid of enforceable standards, the worse the problem will become.

Third, such protections as now exist are in danger of erosion, because of impending interconnectivity between public sector data bases, which are covered by privacy laws, and private sector data bases and transmission systems, which are not.

Fourth, Canadians are entitled to uniform standards of respect for their privacy rights no matter where they live or in what business they are engaged, a situation which can never be achieved if left to the whims of the marketplace.

Fifth, public confidence in any system is unattainable without provision of just rules equally and fairly applied to all segments of society, public and private sector alike, and fortified by a mechanism for independent oversight and complaint resolution—in short, a traffic cop.

Holding the system accountable

Lest we be deflected by uninformed arguments about creating "massive bureaucracies" and "armies of government snoops", let's examine some recent experience. Less than two years ago, the Quebec legislature amended its privacy laws to extend their reach to cover private businesses in the province. The Quebec Commissioner reports that the transition has taken place smoothly, business continues to be done, the sky has not fallen, no-one has complained about excessive or unwarranted intrusions by government snoops. And the bureaucratic explosion? The Commissioner, although he has received about 300 complaints involving the private sector, has added fewer than half a dozen persons to his staff.

For that matter, this Office in its twelve-year lifetime has investigated about 10,000 complaints covering more than 110 government departments, agencies and tribunals, yet has never had a staff of much more than about three dozen persons. In addition to those investigations, this small staff has audited the information management practices of roughly a third of the government's operations, and conducted active research, policy and public affairs programs. So much for bureaucratic bloat.

Another argument gaining some currency is that each sector of the commercial world should have its own privacy watchdog, e.g., the Canadian Radio-Telecommunications and Television Commission for the communications sector, the Canadian Transportation Commission for transportation, the Office of the Superintendent of Financial Institutions for the banks, and so forth. Unless people are willing to discard all their concerns about bureaucratic growth, level playing fields and uniform standards, these arguments should get the quick dismissal they deserve. Not a single jurisdiction in the world where business is governed by privacy laws (and that includes most of Western Europe, Britain, New Zealand and Australia) has ventured down that thicket-strewn path.

The danger of having various industry privacy agencies is the tendency to develop cultures highly reflective and sympathetic to the industries they regulate. There must be genuine independence of thought from those whose interest, first and foremost, is privacy. We do not have separate police departments for each offence but one department with several specialties. The police act on behalf of the whole community and are expected to apply a common standard equally across the whole of that community.

Charting the course

Therefore I put the simple proposition: if the world is changing in ways which threatened established and accepted rights, then so must change the laws which are needed to fortify and defend those rights.

The conclusions are inescapable:

- privacy protection cannot be left to the whim of the marketplace, but deserves and needs to be re-enforced by legislated standards;

- legislation must cover both the public and private sectors;
- action is needed at both federal and provincial levels, and steps must be taken to seek the maximum attainable harmonization of law and enforcement;
- legislated standards must be supported by an independent oversight and compliance mechanism, without which the standards would be merely ineffectual statements of good intent;
- the social and technical impact of information technologies needs systematic assessment by an independent, expert body similar to the U.S. Office of Technology Assessment.

Both provincial and federal governments occupy important jurisdictional positions in the information world. Ideally, both levels would implement complementary legislation more or less simultaneously, supported by similar oversight methods, resulting in uniform and complete coverage of the Canadian information spectrum. Realistically, such an outcome is likely to demand far more time than the urgency of the situation demands. Technology continues its onward rush; if none acts until all act, much that could be saved will be lost.

No time to take our time

Given the national nature of the problem, the responsibility naturally falls upon the national government to exercise leadership. It is a fortunate happenstance that some of the major sectors of commerce fall within federal jurisdiction. These include telecommunications, transportation and banking, three of the most important sectors to collect and use personal information. The federal government thus has the opportunity to seize the initiative and, acting within its own jurisdiction, make the federally-regulated private sector subject to the federal *Privacy Act*—as it is subject to federal human rights, official languages and labour laws.

This action could be supplemented by adding to the *Privacy Act* provisions specifically tailored to the private sector, such as the model privacy code developed by the Canadian Standards Association.

This second option has some appealing advantages. It would embody in law a set of rules devised by a committee representing a broad cross-section of Canadian private enterprise. The major improvement between the situation today and the one this approach proposes is that observance of the CSA standards would become a legal obligation and would be supported by a system of independent oversight. A further advantage is the potential for provincial acceptance, since the enterprises represented on the CSA committee operate in both jurisdictions. In addition, the code has won the endorsement of several provincial privacy commissioners as an excellent basis for legislation. Thus we have at hand a set of privacy rules which, given the necessary teeth, already enjoy substantial acceptance at both federal and provincial levels.

In summary then, the federal government should strengthen Canadians' privacy protection by

- extending the *Privacy Act* to those areas of the private sector which fall within its jurisdiction, and
- convening a federal provincial working group to seek harmonization of privacy laws in the private sector under provincial jurisdiction.

To end at the beginning, the tide is at the flood. Let's not miss it.

On such a full sea are we now afloat,
And we must take the current when it
serves,
Or lose our ventures.

—Julius Caesar, Act IV, Scene III

Update: Privacy, Security and the Information Highway

Few subjects have spilled more ink or prompted more sound bites during the past year than the information highway. Lost in the hype was the Information Highway Advisory Council's call on the federal government "to act to ensure privacy protection on the information highway".

The council is a joint industry/consumer/academic group appointed by the federal government to develop a strategy for Canada's information highway. Among the issues it examined were protecting privacy, and a related concern—protecting security of interactive systems and the data they carry.

Privacy and security are not the same, of course. The distinctions are important—a secure data network may protect against intrusions by unauthorized users but it offers the subjects no protection against overzealous collection and misuse of their personal information, nor against inappropriate disclosures by the controllers and authorized users.

Protecting privacy

The council's discussion paper, *Privacy and the Canadian Information Highway*, set out the privacy threats and asked Canadians to comment on the balance between freedom of information and the threat to personal privacy posed by the information highway.

Public responses (including one from this Office) convinced the council that Canadians are worried that their personal, medical and financial records are at risk on the information highway and they want effective privacy protection. The council concluded that the federal government had to take the leadership in protecting personal information.

Although its final report is not expected until this fall, the council has already acknowledged publicly the need for a national standard—covering all the public and private sectors—to protect Canadians' privacy in an electronic environment. To accomplish this, the council recommended

- establishing a level playing field by developing national, flexible privacy framework legislation to set a minimum fair information standard, and citing the Canadian Standards Association draft "Model Code for the Protection of Personal Information" as that standard;
- establishing a federal-provincial-territorial working group to implement the principles across Canada;
- updating and harmonizing the government's own privacy protection policies, legislation and guidelines;
- setting up a working group to coordinate the development and application of privacy enhancing technologies for delivery of government services and information.

Particularly heartening is the council's recognition that while voluntary standards are useful for engaging business in privacy protection, government must pursue development of effective oversight and enforcement mechanisms, otherwise what becomes of clients of companies that decline to "volunteer"?

Ensuring security

Security is a critical issue in interactive networks, to protect both stored data as well as personal and business communications.

Nevertheless, the council recognizes that no security measure or technology can offer absolute protection for information. It recommends a basic level of security that "provides a reasonable expectation that private communications and personal information will be protected". The market would be left to devise and sell enhanced security protection for more sensitive data.

Striking the right balance between privacy, civil and human rights, law enforcement and national security on the information highway will require extensive study and public consultation. One method of securing communications and data on the highway is to build a public key infrastructure.

In the interests of starting the debate, some definitions are in order.

From post box to E-mail to public key infrastructure—a primer

Security of the mail has long been critical to public trust in the postal service. We expect our mail to be delivered to the addressee in a way which ensures the confidentiality of the message. We seal it in an envelope and entrust it to a postal system which collects, routes and delivers the communication.

Essential to the process is our knowledge that the system is confidential and protected by law. No matter how many truck drivers, sorters and letter carriers handle a letter, we rely on the system to deliver it to its destination unread, unaltered and intact.

Electronic Mail or E-mail is simply a communication sent electronically by connected computer systems rather than by letter mail. But electronic mail offers no sealed envelopes to protect confidentiality or trusted system to ensure safe delivery. Neither the sender nor the recipient has any control over (or knowledge of) who reads their E-mail while in transit. A message sent in the open over a computer system means anyone with access to the system can read, record, monitor, tamper with or destroy the communications before it arrives at its destination.

One solution to protecting E-mail is encryption, and, to confirming the source of messages, authentication by digital signatures.

Encryption

Encryption renders a plain text message unintelligible to all but the intended recipient who has the key to decipher the code. The message is encrypted using mathematical processes, called algorithms, to transform plain text into cipher text and vice versa. Algorithms are simply coding systems for concealing the meaning of a text—analogous to conventional locks.

Along with algorithms, encryption also uses keys. Keys can be numbers, characters, or phrases (in the form of digital bits) used by an encryption algorithm to lock or unlock the transformed message. The encryption key fits with the algorithm to lock or unlock it.

Secret key v public key encryption

Two encryption methods are popular today: the secret, shared single-key type and the public/private two-key type.

In a single, shared key system, both the sender and the recipient must share the same, secret key to either encrypt or decrypt the message. The drawback of this traditional system is that the sender and recipient must share the key with each other. When there are many correspondents, the sender must share a different key with each of the intended recipients and all must be kept securely.

The second method, known as public key cryptography is based on having an associated pair of keys: a public key (known to many) to encrypt the data; and a private key (known only to one party) to decrypt the data. While the keys make a matched pair, one cannot derive the private key from knowing the public key.

In this system, someone wanting to receive confidential information can distribute their public key widely; for example, in a directory. Anyone wanting to send a protected message to that person could look up his or her public key and use it to encrypt their message. The message could only be decrypted by the person holding the corresponding private key. No one else, not even the person who encrypted the message, could decrypt it.

Digital signature—identifying the sender

Electronic communication systems must also be able to authenticate both the sender and the message. A handwritten signature serves as tangible proof of the origin of a conventional letter (a signature can also differentiate an original document from a copy) but one cannot physically sign an electronic document—merely indicate who it is from.

Electronic messages can be altered, or the sender simply masquerade as someone else. Several politicians have recently had electronic words put in their mouths on electronic chat groups and bulletin boards. Electronic communications require that trusted digital equivalent of a handwritten signature.

Public key encryption can provide that trusted signature by reversing the roles of the public and private key. The sender simply encrypts the message with the recipient's public key and attaches a signature block encrypted with his or her own private key.

The recipient can open the message in the normal way with his or her own private key and also verify the sender's identity by decrypting the signature block with the sender's public key.

Appending a signature block that has been encrypted with the sender's private key is like signing and sealing the document. Only one person is associated with that particular private key; the identity can be verified by the corresponding public key and cannot be denied.

Authenticating the message—the "hash" code

Along with the signature block, the sender's encryption program also creates a unique mathematical summary or picture of the message being sent. This is called a "hash code". The recipient's encryption program reads the message, creates the hash code of the message received (a "rehash") and compares it with the hash code in the sender's signature block. If the two codes match, the message has not been altered.

Building a public key infrastructure

Encryption protects the confidentiality of E-mail and digital signatures prove the origin and authenticity of the message. Used together, they can provide electronic privacy.

But one question remains: Who will be the trusted delivery and address system—the equivalent of the traditional postal service? How do we obtain our public/private key pair, how can we be assured that a certain public key is linked with a certain individual, and how do we get each other's public key?

The answer lies in creating a trusted authority to generate the key pairs, to certify the validity of those keys, and to manage the secure distribution of the keys. In short, this means a central administrator to vouch for the identity and validity of the public/private key users and to maintain system security. The authority must also provide key management, such as producing a directory of public keys to ensure that users have access to one another's public keys, and issuing public notices of compromised or revoked keys.

The federal government has recognized the need to develop an infrastructure and has taken preliminary steps to assess departmental needs, propose a concept of operation and work with the private sector to develop a model and uniform standard.

However, vigorous public debate is needed before the government hands any agency the keys to the kingdom.

Update: A Model Privacy Code for the Private Sector

The most ambitious attempt to protect privacy in the private sector has been the Canadian Standards Association's work to produce a model code for Canadian business. The CSA initiative brought together a working group of disparate private and public sector representatives to devise a privacy standard to which all could subscribe.

The members include representatives of public and private sector users of data, organizations representing the data subjects (employees and consumers), the technology industry, and the federal and Ontario privacy commissioners.

The work has been hard but there has been considerable success. The group circulated its first draft for public comment on December 31, 1994 and the verdict is in. The code's statement of fundamental principles is at least as good as—and arguably better than those contained in the *Privacy Act*.

The first principle makes each organization responsible for the personal data under its control and requires it to designate an individual to be accountable for its compliance with the fair information principles. These are identifying the purposes for collecting information, ensuring the individual is informed and consents, limiting collection and gathering by fair and lawful means, limiting collection, use and disclosure, ensuring accuracy, protecting the data, making its personal information handling policies and practices "readily available", providing individuals access to their personal data and establishing their right to challenge its accuracy and completeness, and providing individuals with the means to challenge the organization's compliance with the principles.

The code is thorough and complete, and it was conceived by the private sector to be relevant to the private sector. This is a hopeful beginning.

The Office embarked on the CSA project four years ago, committed to support any scheme that would meaningfully advance Canadians' privacy rights. A model voluntary code was in keeping with the times. But as the threats from technology evolve, so must the

solutions. It is evident that a self-regulatory and entirely voluntary code is out of step with both the enormous social implications of technological change, not to mention rising public concern. Depending on an entirely voluntary privacy scheme in an era of Internet, Pharnanet, electronic wallets and smart cards requires a suspension of belief.

Statements of good intent are no longer good enough. Canadians need and deserve better. Anything less than enforceable privacy rights and independent oversight will be ineffectual. Stacking an individual's privacy rights against the potential economic returns of, for example, database marketing is, at best, an uneven fight. Voluntary codes not only deprive the public of legal protection, but may well deceive us into relying on a chimera.

The greatest significance of the CSA Code may lie, not in its proposed form as a voluntary code for business, but in its embodiment into national framework legislation—a national standard of privacy protection against which all sectors can be held accountable. The Information Highway Advisory Council has recognized the code's place as the basis for legislation, coupled with an effective oversight mechanism. The Commissioner can only applaud.

However, the bottom line is that the rules must be clear, everyone must play by them, and they must be enforceable. Optional privacy protection is simply not good enough.

Update: Biomedical Privacy

The watch on drug testing

The watch on federal government drug testing schemes continues. Mandatory drug testing, lauded as the quick fix to employee drug abuse, is a serious privacy intrusion—surrendering a bodily substance to allow others to ascertain one's past behaviour.

The invasiveness of the procedure and its overtones of surveillance demand that advocates of testing (and there are many) justify the intrusions by demonstrating that drug abuse is a problem in the workplace, that drug testing achieves some valuable objective such as increased safety, and that other, less intrusive, measures would not.

Some have read the position as somehow supporting use of illicit drugs. Hardly. The message is clear—dealing effectively with drug abuse requires education, support, treatment and, in some cases removing workplace conditions that may well cause or exacerbate employees' problems. Massive mistrust of employees and finger-pointing are not the answer.

National Defence drops random tests

One of the first tests of the Office's position came in a May 1992 Order-in-Council authorizing the Department of National Defence (DND) to conduct a broad range of testing programs on members of the Canadian Forces. The program included random testing for deterrence, post accident, suspected cause and as part of a drug-related probation or treatment program. The program targeted illegal drugs, not alcohol, the most widely used and, one might argue, the most frequently "abused" drug in the Canadian Forces.

A thorough analysis of members' drug and alcohol use, using DND figures collected from its 1989 Canadian Forces lifestyle survey, showed that, like their civilian counterparts, Forces members rarely report using illegal drugs. About six per cent of Forces' Members used marijuana within the last year, slightly less than the public at large. However, members drink more frequently; 84 per cent of members reported having a drink in the past year, compared with 78 per cent of the Canadian public.

Since DND's own survey failed to demonstrate that its members had a serious problem, the Commissioner wrote to the Chief of the Defence Staff early in 1994 opposing widespread random testing of Forces' members.

In February 1995, current Chief, General A.J.G.D. de Chastelain, wrote to advise that he had indefinitely suspended the random testing component of the program—one of its most objectionable features. He reserved the right to "reopen the issue if future circumstances dictate".

This is an important event in the annals of Canadian drug testing. General de Chastelain's decision to suspend random drug testing is a blow for common sense and sets an example for public and private sector organizations contemplating drug testing as the "fix" for perceived workplace problems.

DND will rely on education and counselling but will continue testing following an accident to determine whether alcohol or illicit drugs were a factor. DND's own reports found that drugs were not a factor in any of the nine accidents investigated over a two year period.

Dusting for dope

The news is less promising in the private sector. In late March, an American company launched a home drug testing kit—"Drug Alert"—targeted at worried parents and suspicious employers.

The kit contains a piece of pre-moistened cloth that can be wiped across doorknobs, desk-tops and clothing to pick up traces of illicit drugs. The cloth is then placed in a sealed envelope and returned for analysis. The company promises to detect the presence of about 30 illegal drugs.

Assuming the testing process is accurate, the information it produces is ambiguous. The test does not confirm that the person used drugs; it merely shows contact with traces of a drug which could be completely innocent. Contact with other drug users could leave a residue sufficient to generate positive test results. Anyone who handles American (and likely Canadian) paper money may pick up traces of cocaine, given the bills' frequent use as straws for inhaling the powder.

The most disturbing aspect of the kit is its marketing to capitalize on parents' understandable fears of childrens' use of drugs. American "war on drugs" rhetoric spills over the border, misleading parents into believing there is an epidemic of drug abuse among Canadian students. Some students are indeed using illicit drugs but recent statistics demonstrate that while the levels of use fluctuate, all are down from the rates in the 1970s.

The kit is a device for spying on children and a surreptitious invasion of privacy. The consequences of error for parent-child relationships could be fatal. We once feared invasions of privacy by the state, then by the private sector. Must we now fear our own family?

There appears to be no federal law preventing such surveillance. Several provinces have statutory privacy torts and Quebec's Civil Code and human rights charter protects citizens against spying. Parents who choose to invade their children's privacy and betray their trust this way could find themselves facing a civil lawsuit. They could also find the tables turned. Having had their own trust betrayed, children could try the tests on their parents. Is this the course we want our society to follow?

There is also evident appeal to employers. Unlike urinalysis, this type of test does not require the knowledge or consent of the employee and need never attract the attention of human rights bodies. The Commissioner's strong objections to urinalysis pale beside those about secret drug testing. Although he has no legislative authority to prevent such testing, he is not afraid to lead the chorus for laws against its use.

DNA testing in criminal investigations

There has also been significant progress on the DNA testing front, specifically legal controls on forensic DNA tests.

If nothing else, the O.J. Simpson trial has brought this once-arcaic technology into the living rooms of the nation. Forensic DNA analysis is a valuable identification tool which can help convict or exonerate individuals suspected—or even convicted of a crime. The most recent Canadian example of its use is the case of Guy Paul Morin. Mr. Morin had been accused and convicted of the sex-related murder of a

child. Late in January 1995, advanced DNA testing proved conclusively—ten years after his arrest—that he had been wrongly convicted.

However, the intrusiveness of this technique warrants careful regulation of the circumstances in which a criminal suspect should be required to supply DNA.

The federal government recognizes the power of this evidence and need for its regulation. With this report in the final throes of preparation, the House of Commons passed Bill C104 amending the *Criminal Code* and the *Young Offenders Act* to allow forensic DNA testing. The Bill is before a Senate Committee. Once passed, it will provide a legislative framework for taking and using DNA in criminal investigations. (Still to come are amendments governing establishment of DNA databases.)

Although the legislation appeared—at least to the public—to have been thrown together in a hurry, in fact the Department of Justice issued a consultation paper in September 1994 on obtaining and banking DNA forensic evidence. The paper paid considerable attention to the privacy implications of DNA analysis, capturing many of the recommendations in the Office's 1992 report, *Genetic Testing and Privacy*.

In January 1995, the Office responded to the Justice consultation paper, acknowledging the utility of forensic DNA analysis but entering several caveats. Bill C104 deals with, or undertakes to deal with most of these in a final round of amendments, promised for later this year. The amendments will address the storage and use of the samples (or their analysis).

Many of Bill C104's rules on collecting and using DNA samples mirror the Office's recommendations. For example,

- a judge must authorize the collection from the suspect;
- testing is limited to a series of "designated offences", primarily sexual and/or crimes of violence;
- a DNA sample must be relevant to proving the offence, investigators must have DNA from the crime to compare with the suspect's sample;

- analysis of the samples are to be used only to confirm or negate a match between samples from the crime scene and the suspect;

- DNA samples (and any analysis of that sample) must be destroyed immediately if the accused is acquitted, or within a year if the Crown does not proceed with a charge, withdraws the charge or enters a stay.

Some of the Office's recommendations were not specifically incorporated in the current bill. The most important of these is rules establishing whether, how and for how long authorities keep the actual sample or only the analysis of the sample. The Minister has undertaken to deal with the important and sensitive issue of banking the samples or the analysis in subsequent amendments to be introduced later this year. Also needed is a provision establishing defendants' rights to get access to samples from the crime scene to allow for independent testing.

One of the remaining issues concerns police matching the analysis of a sample obtained under a warrant for one crime, with samples gathered at other crime scenes. We look forward to discussing rules for storage and subsequent uses of the data at the second round of amendments. This issue is simply too important for any misunderstanding.

A model genetic Privacy Act

Bill C104 is cause for cautious optimism. But controlling forensic uses of DNA is just the first step. We are less optimistic about the prospect for protecting genetic privacy in other areas—among them employment, insurance and human reproduction. The time may be right for other federal departments and indeed, all governments, to turn their minds to regulating these other collections and uses of DNA analysis.

The publication by Boston University School of Public Health early this year of a model "*Genetic Privacy Act*" may kick start the process in Canada.

The drafters of the model legislation offered this summary of its philosophy:

[T]he overarching premise of the *Act* is that no stranger should have or control identifiable DNA samples or genetic information about an individual unless that individual specifically authorizes the collection of DNA samples for the purpose of genetic analysis, authorizes the creation of that private information, and has access to and control over the dissemination of that information.

The rules protecting genetic privacy must be clear and known to the medical, scientific, business and law enforcement communities and the public. The purpose of the Genetic *Privacy Act* is to codify these rules.

The Genetic *Privacy Act*, though drafted for an American audience, contains much that could be carried into Canadian law. Armed with this legislative template, Parliament has even less excuse for delay in addressing the increasing threat to our genetic privacy.

Update: Safeguarding Tax Files

There are now stringent safeguards on using taxpayer information for monitoring Taxation employees, thanks to the efforts of Revenue Canada, the Union of Taxation Employees and the Office.

A union representative wrote to the Commissioner setting out members' misgivings about proposed amendments to the *Income Tax Act* and the *Excise Tax Act* (see 1992-93 report). Their concern centred on broad proposals allowing Revenue Canada to use taxpayer information to supervise, evaluate or discipline its employees. This would subject Taxation employees to harsher monitoring than other federal employees and diminish taxpayers' confidentiality by allowing Revenue Canada to use their tax files for purposes unrelated to filing a tax return.

Taxations' need to ensure the integrity of the tax system was not in question. But the proposals were drafted so broadly that there was potential for abuse. Setting out these uses in the *Income Tax Act* overrides a provision in the *Privacy Act* which prohibits using information obtained for one purpose (filing tax returns) for another purpose (supervising employees). The Commissioner wrote to Revenue Canada and the House of Commons Finance Committee recommending stringent safeguards.

Revenue Canada offered to prepare draft guidelines establishing criteria and setting out controls for managers wanting to examine taxpayer and employee tax files during an investigation. They also offered to have the Office review the draft. Staff made several suggestions and the guidelines are now final. They include:

- not examining an employee's tax return as part of the annual performance review;
- protecting the confidentiality of taxpayers' returns used as evidence during grievance or arbitration procedures;

- requiring an assistant deputy minister's authorization to use a tax return in an investigation of suspected serious breaches of either act (such as using insider information for personal benefit or altering a return to benefit or hurt someone else);
- establishing an audit trail by keeping records of requests and supporting reasons in the security division;
- protecting the confidentiality of taxpayers whose tax returns are used as evidence in legal proceedings against employees (for example, by banning publication of those records, concealing the taxpayers' identities, or hearing selected evidence *in camera*).

The deputy minister also agreed to have employees notified each time a director requests access to their tax returns.

The Office will audit compliance with the guidelines.

Update: The Privacy Patchwork

In Canada...

In June 1994, **Alberta** passed its long-awaited access to information and privacy law. Beginning October 1995, the *Freedom of Information and Protection of Privacy Act* will provide Albertans with access to general government records, as well as to their personal information held by the government, municipal agencies, universities, school boards and health care agencies. The *Act* will also protect Albertans' privacy by establishing controls on provincial ministries' collection, use and disclosure of their personal information. The commissioner (who is also the provincial ethics commissioner) is responsible for investigating complaints and monitoring compliance and has the power to make binding orders.

By September 1994, the government of the **Northwest Territories** had also passed its *Access to Information and Protection of Privacy Act* to open its agencies' records to public access and give territorial residents the right to access and request correction of their personal information held by these agencies. The *Act* will come into force in December 1996. Its controls on the collection, use and disclosure of personal information by territorial agencies brings the Northwest Territories in line with the rest of the country's privacy protection regime. Complaints will be investigated by an ombudsman.

The revised **Nova Scotia** *Freedom of Information and Protection of Privacy Act* came into force in July 1994. The *Act*, the fourth version of the *Freedom of Information Act* since 1977, is the first to include specific provisions protecting the privacy of provincial residents by controlling provincial government collection, use and disclosure of their personal information. Nova Scotians also have the right to access and request correction of their personal information held by ministries, municipal agencies, school boards and universities. Complaints are handled by a government-appointed Review Officer.

Prince Edward Island is now the only province or territory without any form of access to information, privacy or data protection law. However, following the March 1994 provincial throne speech, a legislative committee looked into the need for a freedom of information and privacy law. The committee recommended adopting such a law and its report includes suggested wording, apparently inspired by the Alberta legislation. If the government adopts the committee's recommendations, Prince Edward Island could fill the last hole in the public sector patchwork as early as 1996.

Of course, the private sector remains unregulated, except in Quebec.

...And Abroad

The **European Union** Council of Ministers adopted its *Directive on Data Protection* on February 20, 1995 and has referred it to the European Parliament for ratification. The directive, first proposed in September 1990, spells out rules to protect Europeans' privacy and to control the processing and flow of their personal information. Clause 25 of the directive may pose some difficulties for Canadian companies doing business with Europe because it prohibits member countries from exchanging personal information with non-member countries lacking adequate data protection laws. With the exception of Quebec, Canada has no privacy legislation protecting personal information held by the private sector, and proposed voluntary codes do not meet the directive's adequacy test.

In the Courts

Privacy and Access of equal weight

The Federal Court of Appeal, in its recent decision in *Minister of Finance v. Michael A. Dagg* (A-675-93), confirmed that the *Privacy Act* and the *Access to Information Act* have equal status and that disclosure of personal information under the *Access Act* is subject to the provisions of the *Privacy Act*. Given the implications of the trial judgment—second class status for the *Privacy Act*—the Privacy Commissioner intervened.

Mr. Dagg, a private consultant, asked the Minister of Finance to provide him with employees' after-hours sign-in sheets for specific days between September 1 and 30, 1990. He wanted to determine how many members of the Economists, Sociologists and Statisticians Association (ESSA) worked overtime on a regular basis. Dagg intended to calculate the total number of hours worked and sell this information to ESSA for use during the next round of collective bargaining. The Minister provided him with a copy of the sheets requested, but deleted the names, identification numbers and signatures of the employees.

Mr. Dagg complained to the Information Commissioner, who agreed that the details were personal information. Dissatisfied, Mr. Dagg appealed the department's decision to the Federal Court. Mr. Justice Cullen concluded that the information was not personal but of a "predominantly" professional nature. He stated that government institutions were only bound to protect information whose predominant characteristic is of a personal nature. He added that "when there is any doubt as to whether information constitutes "personal information" which should or should not be released to members of the public, the benefit of the doubt is to be given to the interpretation which favours disclosure...".

The Minister of Finance appealed the decision to the Federal Court of Appeal.

The Chief Justice, writing for the Court of Appeal, overturned Mr. Justice Cullen's decision. The Court stated clearly that both statutes should be construed on the same footing. Both must be read together since section 19 of the *Access to Information Act* incorporates by reference certain provisions of the *Privacy Act*. Nothing in the language of either statute suggests that one is subordinate to the other. They are

complementary and must be construed harmoniously in order to attain Parliament's objectives.

As for the "predominant characteristic" test, the Court held that it is clearly wrong, since it amounts to an unwarranted attempt to amend the definition of personal information in section 3 of the *Privacy Act*. The Chief Justice pointed out that the definition is broad, enlarged by nine classes of information or illustrations and four classes of exceptions. Information is either personal or it is not—there is no class of predominantly personal or predominantly non-personal information. Whether an employee is at a particular place at a particular time is information personal to that employee.

Denied adjudicators' notes—case goes to court

The Privacy Commissioner has taken a second case to the Federal Court (the first case was settled on the courthouse steps). He has asked the Court to review a Canada Labour Relations Board (CLRB) decision to deny a complainant access to Board members' notes.

The complainant had taken a complaint against his union to the CLRB which hears industrial relations disputes from organizations under federal jurisdiction.

Dissatisfied with the Board's decision, he asked to see the panel members' notes. (Although Board hearings are public, the proceedings often are not recorded—and were not in this case.) The Board refused to process the notes under the *Privacy Act*, considering they belong to panel members. The notes are not kept in CLRB files and, therefore, the Board argues that they are not under its "control".

The Commissioner considers the notes are taken as part of an administrative process. They are not the personal property of board members but are prepared to fulfil their duties and so are under the control of the CLRB. The *Act* gives individuals the right to know what information is held about them in organizations subject to the *Privacy Act*.

The Commissioner's application asks the Court to order the CLRB to review the notes under the *Privacy Act* and to provide the complainant with access to his personal information, subject to any exemptions.

The hearing is expected to be held in the fall.

Consulting the Commissioner— MPs' pensions

Departmental staff often call the Office to discuss balancing the public's right to know and an individual's privacy. A recent case illustrates the murky depths beneath what appears to be a placid surface.

"Letting the facts get in the way of a good editorial"

A political debate continues to swirl around the alleged profligacy of federal MPs' pensions and the Federal Court is now reviewing a department's denial of access to related information. This is a minefield for comment. Nevertheless, some gaps need filling.

In order to pursue the Great MP Pension Debate, an individual asked Public Works and Government Services (PW&GS) to provide "Under the *Member of Parliament Retiring Allowances Act (MPRAA)* as of September 1, 1993, name of current recipients, identity of survivors, total amount paid for each and breakdown of member/government contributions".

The department refused the request, arguing that the information was personal and therefore exempt under the *Access to Information Act* (subject to some specific exceptions). The applicant complained to the Information Commissioner who supported PW&GS' position, with one exception—the names. Since former MPs and their terms of office are listed in public documents, the Information Commissioner recommended the department disclose the names of MPs receiving pensions. Public Works sought this Office's advice.

The Privacy Commissioner's role is not to advise departments when to release personal information. The *Act* clearly makes that the responsibility of the head of the agency who has both an intimate knowledge of the records and is answerable for their care. The

Commissioner simply sets out the factors the department should consider before releasing personal information. Departments have the option of

- seeking the individuals' consent to the disclosure;
- determining whether there is a "public interest" sufficient to outweigh any invasion of privacy, or
- concluding that the information is "publicly available".

The department asked pension recipients for consent to release but many refused. The head did not consider the public interest sufficiently outweighed the individuals' privacy interests and so did not use his discretion to release the information.

"Publicly available"

The argument in favour of disclosure in this case then focuses on the contention that the information is publicly available because names of former MPs could be assembled from the public record—for example, the Canadian Parliamentary Guide and the Canadian Parliamentary Handbook. Indeed the handbook lists serving MPs for every riding in every election between Confederation (or creation of the riding) and 1988. The reader could determine who has accumulated six or more years service and therefore qualified for a pension.

However, this merely establishes MPs' eligibility, not their actual receipt of a pension. There are sufficient variables—buy-back options or return of contributions for breaks in service and the inclusion of hundreds of MPs who have since died—to make the public data incomplete.

The case begs several questions. If the information is already publicly available, why is a Court action—or, indeed, any action—necessary? How will releasing only the names respond to the applicants request? Why are there apparently several versions of the "correct" list? Why would the department be compelled to release a specific list of pension recipients because a general list of former MPs is publicly available? When the names of other surviving beneficiaries (spouses and dependents) are removed, will the list be accurate and complete?

Finally, how does knowing which MPs are collecting a pension help the public judge the appropriateness of the pension plan when all the information needed to assess the plan itself—the breakdown of MPs' and government contributions, interest, disbursements, withdrawal allowances and account balances are already open to public scrutiny?

The department rejected the Information Commissioner's recommendations and the matter is before the Court.

Investigating Complaints

Intake of new complaints recovered from last year's breather and hit an all-time high of 1783. This is an increase of 493 or 38 per cent over the 1290 received in 1993-94. Staff completed 1307 investigations, of which 595 were well-founded, 645 not well-founded and 26 were resolved. The remaining 41 were abandoned or discontinued at the complainants' request.

The increase in complaints can be attributed at least in part to a 78 per cent increase in time limit complaints; in many instances the direct result of staff cutbacks and government re-organization. As well, a quarter of the 729 time limits cases were lodged by four individuals against the departments of National Defence, Revenue Canada and Correctional Services Canada.

Time limits and denial of access complaints continue to make up the majority. However, complaints about improper collection, retention, use and disclosure of personal information ("privacy" complaints) climbed 22 per cent to 348 in 1994-95. Of these, 66 per cent concerned improper use and disclosure, 20 per cent improper collection and 14 per cent improper retention. Use and retention complaints are more complicated to investigate, often require travel (thus demanding more days to complete) and extend overall turnaround time.

Contracting out—an update

Last year's report discussed the Commissioner's concern that individual's privacy rights were being denied when departments contracted out services—the case in point was harassment investigations.

At issue was individuals' access to documents gathered by an individual or company not subject to the *Privacy Act* but performing services under contract for a government institution that is. Some of these contracts specify that consultants are **not** to provide witness statements or other personal details but to deliver only the investigation report. In other cases, consultants have simply refused to disclose the information to the department, maintaining that they have promised the witnesses confidentiality. The legal question is, who has "control" of the records?

There has been progress. In a case this year against Public Works and Government Services, the deputy minister agreed that contractor's notes are under the department's control and to have them reviewed to respond to the complainant's application under the *Privacy Act*.

Informal v formal access

One issue discussed with Correctional Service Canada this year is the method it has established for giving inmates access to their personal information.

Inmates have rights under the *Privacy Act*, including rights of access and correction, and the right to complain to the Privacy Commissioner—and ultimately to the Federal Court, if they believe they have been improperly denied access. However, to benefit from independent oversight, inmates must apply under the *Privacy Act*. CSC processes *Privacy Act* requests formally at ATIP Directorate at Headquarters.

But inmates have another option. The *Corrections and Conditional Release Act* also gives them rights of access and correction to information held by CSC. Generally, CSC encourages informal requests because they are processed in the institution and so speed up the process. Each institution designates a staff member to help inmates phrase their requests. However, there is no recourse to an independent investigator.

Although informal access is praiseworthy, the inmate should have the choice. Institutions should not establish processes that force an individual to forego rights under the *Act* for the sake of expediency. Some inmates will choose the formal process under the *Act*, either because they do not trust the institution or because they want to retain their right of recourse to an independent body.

The "resolved" category

Regular readers will notice a new category of complaint finding this year—the Commissioner considered several cases "resolved". The Office has struggled with past complaints for which "well-founded" appeared too harsh to fit what essentially had been miscommunication or

misunderstandings. The power of an ombudsman's role is the flexibility to solve problems—resolution is an ombudsman's stock-in-trade. Resolved cases are those in which

- there was a misunderstanding or miscommunication between the complainant and department about what information was being sought. Both parties agreed to a mutually satisfactory solution;
- the individual claimed specific information was missing, the department maintained that it had disclosed the records but readily agreed to send it again;
- the department had the right to exempt the information, but was persuaded by the investigator to exercise its discretion to release it; or
- the investigation identified inconsistent processing of large volumes of information for an applicant, and the department was persuaded to release more information to make the disclosure consistent.

The following are selected from the 1307 cases completed this past year.

Counting privacy in—the census

This year saw the Office complete its longest and most labour-intensive investigation—33 complaints about the last census. The results more than justify the time—they led to significant changes planned for Statistics Canada's next census in 1996.

The census is the federal government's most extensive, expensive and potentially most invasive collection of personal information. Many would also argue that it is also the most valuable to society and the economy.

The challenge is to seek a reasonable balance between the value of a census to the nation, and the inherent intrusiveness of any questionnaire. Where does a democracy draw the line between its need for reliable data and a healthy reluctance to compel citizens to provide

detailed information about their race, religion, lifestyle and health for a data collection that is never destroyed?

This debate is broader than the mandate of a privacy commissioner and perhaps one that needs airing. In the meantime, investigators concentrated on the collection, use, retention and disclosure of Canadians' personal data. To prepare, staff examined the history of the census, its justification and uses of the data, and comparable collections in other countries. With information in hand, staff attempted to resolve the 26 outstanding complaints. (The other seven were either not well-founded or discontinued.)

The complaints fell into two broad categories; those concerning the "intrusiveness" of some of the questions, and those alleging that Statistics Canada's confidentiality guarantees were undermined by its collection procedures. First, the questions.

The "intrusive" questions

Most complainants objected to questions about their race, religion, fertility, housing, physical and mental health, or the number of "person(s) living elsewhere who stayed overnight". One woman, under a psychiatrist's care, was so upset by the question about mental and physical health that her husband tore up the form. Other complainants argued that any questions other than to determine the number of persons in the household were outside the definition of a census, and they were under no obligation to answer.

The research revealed that for almost a century the census has been more than a simple head-count. Census data is used to calculate transfer payments to provinces, chart economic and social change, and forecast Canadian society's needs for schools, medical services and highways. Statistics Canada also sells aggregate data (stripped of personal identifiers and combined with the information of at least 100 other individuals) in various electronic formats including CD-ROM, diskettes and magnetic tape. It is also testing making aggregate data available on Internet.

Nevertheless, some perceive the questions as intrusive, particularly for the one in five who receive the long form. Given the personal nature of the data, the ability to link it to individuals, and its permanent storage, there were serious privacy issues.

The Office began a lengthy consultation with Statistics Canada; both parties were determined to deal with the privacy issues without bringing the census to a grinding halt. In an effort to reduce the intrusions, the 1996 census will omit the question about "person(s) living elsewhere who stayed overnight" from both short and long questionnaires. Questions about religion and fertility will be dropped from the long form and two questions about the respondent's dwelling will be eliminated from the short form which will now be limited to basic demographic information.

To respond to the Commissioner's concern that the justification for many of the questions was unclear, Statistics Canada will also redesign the accompanying Guide, making it easier to read and explaining why the information is needed and how it will be used. It will also establish a Census Help Line during the census collection to answer the public's questions about confidentiality and privacy, as well as help callers complete the questionnaires.

Security of the collection process

To deal with complaints that Statistics Canada's collection procedure threatened respondents' privacy, investigators examined census representatives' oath of office, their hiring and training, as well as the procedures for collecting and handling census information.

The 1991 census procedures did seem to pose risks to the security of the information. Statistics Canada's training of census representatives put inadequate emphasis on privacy protection principles or the public's growing privacy concerns. The agency agreed to expand these issues in training for the next census.

Many complainants worried that neighbours serving as census representatives reviewed the completed questionnaires. The complainants had assumed that their answers would be reviewed by a faceless bureaucrat at Statistics Canada headquarters in Ottawa, not someone they knew.

Statistics Canada will try to reduce the chances of census representatives collecting information from someone they know by assigning them to enumeration areas outside their neighbourhood. This can be difficult in rural areas where the best way of ensuring all households are enumerated is assigning someone thoroughly familiar with the area.

Although Statistics Canada will continue this process, it agreed to explain the role of census representatives clearly on both drop-off and mail-back envelopes. Respondents who do not want their information seen by the local representative can have someone else collect the completed return or mail it to the nearest regional office.

Allowing census commissioners and representatives to work out of their homes also worried a number of complainants who thought the prospect of their completed forms on the family dining table seriously undermined the security of the collection. Statistics Canada provides specific instructions to census representatives on protecting the information they collect, and the agency is confident that the representatives are well aware of security responsibilities.

The centralized edit test project

An important project which could eliminate many of the collection irritants is Statistics Canada's test of a centralized edit collection for the 1996 census. In the test area (10 Ottawa-area electoral districts—400,000 individuals) all census questionnaires will be mailed directly to respondents who will then mail their completed forms to district offices for editing and follow up, rather than to the area census representative.

This will eliminate door-to-door drop-off of the questionnaires, the need for census representatives and, therefore, the likelihood of neighbours reviewing completed questionnaires, as well as worries about security in representatives' homes.

Problems with missing or incomplete questionnaires which district office staff cannot resolve by telephone will be assigned to field representatives who are not local. This should reduce substantially the possibilities of having forms processed by a representative whom the respondent knows.

If this pilot project is successful, Statistics Canada intends to use it nationally in the 2001 census.

Other complainants objected to having to share a single questionnaire with other household members. They argued that this effectively forced them to disclose information to others to whom they may not be related. Statistics Canada delivers only one form to keep collection and processing costs to a minimum. While most households do not need—and would probably protest—receiving separate questionnaires, Statistics Canada will offer individual questionnaires to anyone not wishing to share a form.

In summary, the Office has persuaded Statistics Canada to make several significant changes to census collection to reduce the intrusion into Canadians' personal lives. Those changes include:

- eliminating some of the questions from both short and long questionnaires;
- simplifying the questionnaire and guide so respondents better understand the questions and why they are being asked;
- employing, wherever possible, census representatives in areas where they are not likely to be known;
- offering respondents the option to mail their completed questionnaire to a regional office so that local enumerators do not see their information;
- explaining clearly in the accompanying information the role of the local census representatives;
- training and sensitizing census employees to maintain the strictest principles of confidentiality and privacy in all phases of the census;
- modifying the edit and follow-up procedures to minimize the burden placed on respondents;
- establishing a Census Help Line; and
- testing the Centralized Edit System.

The best privacy solution—destruction

One issue that is vital to Canadians' long term privacy is the current procedure of keeping microfilm copies of completed census questionnaires and all other documents that link the responses with identifiable individuals.

The *Statistics Act* absolutely prohibits Statistics Canada from disclosing personal census information to anyone for any reason. Records for censuses before and including 1901 are kept at the National Archives and are available for public research. But documents from all subsequent censuses remain under Statistics Canada control and no one outside that agency—not even the National Archivist—has access.

The best privacy protection would be destruction of all personalized records from the 1991 census (as well as all other census records not already in the public domain) once Statistics Canada has processed the data to ensure its accuracy and quality. This solution would require Statistics Canada to seek an amendment to the census retention and disposal schedule approved by the National Archivist under the *National Archives of Canada Act*.

While Statistics Canada is prepared to destroy the 1991 records, National Archives officials are very reluctant. This issue will take time to resolve.

However, should National Archives prevent Statistics Canada from destroying personalized census data, the Chief Statistician must notify Canadians that their personal data will be kept for indefinite storage, and eventually transferred to the National Archives. Canadians must know why the information is collected, how it will be used, how long it will be retained and to whom it will be disclosed. These are the principles at the heart of the *Privacy Act*, ones the government's most important personal data bank must live by.

De-personalizing census data is the critical element in achieving citizens' full cooperation, as well as a permanent solution to recurring privacy concerns about the census.

Private detectives and "shadow" files—privacy at Canada Post

A letter carrier's allegations about Canada Post's improper collection and disclosure of medical information and denial of access to health and employment records were serious enough. However, they were merely the tip of the iceberg.

While searching the records, the investigator found evidence that Huron Division managers hired a private detective and put the employee under surveillance. The investigator also found a cabinet full of "shadow" files the manager maintained on employees which he considered his own property and not to be reviewed under the *Privacy Act*.

The woman had fallen and hurt her back while delivering mail and made a Workers' Compensation claim. Despite having undergone back surgery, facing a second operation, and a consensus among her own surgeon and Canada Post-appointed doctors about the cause and extent of her injuries, managers doubted her compensation claim. They believed her injuries were caused by earlier car accidents and not the fall. They asked Corporate Security for authority to put her under surveillance outside working hours. They were refused.

Frustrated, they hired a former postal inspector to conduct the surveillance, not only on the complainant but on two other employees who were also under management scrutiny. Although security officials denied any involvement, the investigator established that one of the staff knew the former postal inspector and recommended him to management to conduct the surveillance.

The managers hired the detective (under the guise of other postal duties) to follow and photograph the complainant during her Compensation leave, hoping to prove her back injury was fabricated. When they were unsuccessful, they shredded what they thought was most of the evidence. However, the investigator found photocopies of the surveillance photographs in the Workers' Compensation component of her Occupational Health, Safety and Environment (OHS&E) files.

OHS&E staff denied any knowledge of the surveillance and could not say how the photographs got there. Certainly, they were not there six months earlier when the woman was given access to what she thought was all her personal information.

In fact, the investigator also discovered that she had not been given the entire 165-page Health Care component of the OHS&E files. Canada Post claimed the omission was inadvertent. However, this file contained most of the references to the surveillance.

Canada Post attempted to continue withholding information about the surveillance from this file, claiming that releasing it would jeopardize a lawful investigation (section 22(1)(b)). The Commissioner rejected the exemption.

The investigator also discovered that the complainant's manager in Huron Division had three large volumes—over 750 pages—of personal information concerning her employment, payroll, attendance, grievance, OHS&E and the requests for surveillance. Canada Post had not reviewed the material to respond to the woman's privacy request because the manager maintained that the files were his own personal property. Ultimately the manager was compelled to turn over the files which Canada Post processed and sent to the complainant.

Other complaints about Canada Post's information handling were also justified, including OHS&E collecting medical information directly from the complainant's orthopaedic surgeon without her consent, and departmental officials failing to remove disciplinary documents from the complainant's employment files despite specific instructions in arbitration and grievance decisions.

Canada Post headquarters' officials acknowledged that managers kept their own personnel files for convenience but were unaware that Huron Division was conducting surveillance. They have stopped the abuse. The staff involved were either disciplined or removed, or have resigned. Canada Post wrote to the complainant to apologize for the surveillance and she has gained access to all the available material.

Although there is only one "official" set of personnel files at Canada Post, many managers keep personnel records in their offices for administrative purposes. Canada Post's failure to review these records to respond to employees' access requests is a source of repeated complaints to—and repeated reminders from—the Commissioner's Office. While

these files should mirror official files, employees wanting access should specify that they want all material searched—including any managers' files—just to be certain.

The Privacy Commissioner considered all but two of the 15 complaints well-founded.

RCMP can notify employers of employees' arrests—properly

Three individuals complained that the RCMP improperly disclosed their arrests to their employers.

In the first case, an RCMP officer disclosed details about the complainant's arrest to the Matsqui penitentiary where he worked. In the other case, a constable notified a bank manager that two of his employees had been arrested for shoplifting.

The RCMP defended the officers' actions, claiming it was in the public interest to ensure employers knew of employees' arrests and pending charges. The RCMP believed that the correctional employee's security clearance might be affected, and that the bank employees may have held positions of trust.

Nevertheless, the Privacy Commissioner considered the complaints well-founded for several reasons.

First, the RCMP failed to follow the procedure for public interest disclosures set out in the *Privacy Act*. Only the most senior officials in an agency should make the decision to release personal information "in the public interest", and then only after carefully weighing whether the public interest "clearly outweighs" any invasion of the individual's privacy. The government is also required to notify the Privacy Commissioner prior to the disclosure, giving him an opportunity, if appropriate, to alert the person to the impending disclosure of their information.

Second, the RCMP has its own procedures for informing employers that employees' actions may have undermined their reliability. They were not followed. Rather, staff in the local detachment made the determination without first obtaining approval from senior headquarters staff who are authorized to make such decisions.

Third, in both instances, the information was not yet a matter of public record. Had detachment staff waited until charges were laid, the disclosure may have been allowed.

Contractor refuses to turn over notes

Recent annual reports have reminded departments not to contract out their privacy responsibilities when contracting out work. The contractor is simply an agent of the department. Any personal information it obtains or prepares belongs to the department and is protected by the *Privacy Act*. That means making it accessible to the person it concerns, protecting it from unauthorized disclosure, making it available to the department to audit contract compliance, and respecting retention and disposal criteria at the end of the contract.

Despite repeated cautions, applicants continue to have difficulty getting access to personal information collected under contract.

For example, a woman recently sought the Office's help to obtain supporting documents collected by a contractor hired by National Defence (DND) to investigate her complaint of sexual harassment. Although DND gave her a copy of the final report, it did not contain a list of witnesses interviewed, the questions asked, and their responses.

The investigator found DND had no supporting documents. He asked DND to have the contractor turn over the documents in order to meet its obligation to provide the complainant access to her information. The contractor refused in order to protect the witnesses' identities.

The Commissioner was willing to pursue the matter but the complainant wanted no further action. Nevertheless, the Commissioner intends following up several similar outstanding complaints against DND (among others) and to obtain the contractors' documents for the complainants. The complaint was well-founded.

Elections Canada to end use of military numbers

Two Canadian Armed Forces' members complained that their military service numbers had been included on mailing lists used by political candidates during the 1993 federal election campaign. Both noticed that the mailing label on campaign literature from their local candidate included their service number.

The investigator established that DND provided Elections Canada with the name, military number and postal address of all eligible CAF members under authority of the *Canada Elections Act*. Military members may select a permanent place of residence (often where they enlisted) or their current posting address. The Chief Electoral Officer must then provide this information to the returning officer of the selected riding, who makes it available to district candidates, on request.

Since there is clear legislative authority for DND to disclose the military service numbers to Elections Canada, and for Elections Canada to disclose the numbers to political candidates, the complaint was not well-founded. Nevertheless, the Commissioner was concerned that providing military service numbers seemed an unnecessary invasion of privacy since Elections Canada acknowledged they were not absolutely required. Elections Canada agreed to seek an amendment to the *Canada Elections Act* to eliminate the need for DND to provide the number. This will be one of a number of amendments expected to be introduced during this session of Parliament.

Tenants' income revealed to justify rent subsidy

Two complainants questioned why their housing cooperatives collected and then gave CMHC detailed information about their income in order to demonstrate that tenants were entitled to rent subsidies.

The co-ops provide accommodation for low and moderate income families and individuals. Tenants who qualify for subsidy pay a percentage of their income as rent; CMHC pays the remainder. CMHC also helps finance a project's mortgage.

In one case, members of a Vancouver cooperative challenged the project's right to request copies of tenants' income tax assessments. The project manager argued that the co-op needs sufficient proof of income to justify CMHC subsidizing tenants. Since there was some suspicion that some tenants were not reporting their true income, he argued that income tax assessments were the most prudent and reasonable means of verifying income.

The second person complained that during an audit of a Scarborough, Ontario co-op, CMHC auditors took away a complete list of all tenants whose rent was in arrears, including the amount of arrears, as well as a printout of rent payments made by all tenants.

CMHC enters agreements with non-profit groups to subsidize non-profit housing under the *National Housing Act* (NHA) and its regulations. The agreements require co-ops to gather information about the financial status of subsidized tenants to justify the CMHC subsidy and to maintain proper evidence to support CMHC's audits of tenant subsidies.

The Commissioner concluded that CMHC was authorized by the NHA to obtain sufficient information (and relevant copies) about tenants and their income status to determine their qualifications for subsidy. The collection was a logical balance between the individual's right to privacy and CMHC's right to be satisfied that the financial assistance it was providing was justified and reasonable. The complaints were not well-founded.

Immigration and Refugee Board needs immigration files

An immigration lawyer questioned the amount of information Immigration and Refugee Board can legally obtain from Citizenship and Immigration Canada about applicants for refugee status. He also challenged the Board's powers to review information about other family members during its assessment of a claim.

The Board demonstrated that assessing refugee claims is part of the overall immigration process and, as such, it has the right under the *Immigration Act* to review personal information collected by Immigration before deciding the refugee's claim. Exchanging personal information

with Immigration Canada is consistent with the purpose of the original collection and so meets the requirements of the *Privacy Act*. The *Act* prevents disclosing personal information without the individual's consent unless that is the original purpose or consistent with that collection.

The Commissioner concluded that it was reasonable for the Board to consider information about other family members when reviewing an applicant's refugee claim. IRB must often verify information when, for example, a claimant is less than honest or the Board suspects the claimant is making multiple bogus refugee claims.

The complaint was not well-founded.

Balancing privacy and spiritual beliefs

One of this year's complaints illustrated a potential clash of individual rights—the privacy rights of female correctional officers and the spiritual beliefs of Aboriginal inmates.

A Member of Parliament complained that one of his constituents, a corrections officer at the Saskatoon Regional Psychiatric Centre, had been asked to notify her supervisor when she was menstruating. The woman said that she had first been approached by two Aboriginal resource staff while she was guarding a sweat lodge ceremony during the first visit of a traditional healer. The resource staff explained that Aboriginal cultures believe a woman's menstrual period intensifies those powers normally associated with procreation. Proximity to these increased powers are believed harmful to men and sacred items in the sweat lodge.

According to the complainant, when she told her supervisor about the incident, he asked her to advise the manager on shift when she was menstruating so she could be re-assigned.

The investigator was unable to confirm either conversation. The resource staff denied having broached the subject with the woman. And the supervisor denied having asked for the information. He said he simply offered to have her report to a female manager and be assigned to other duties, should she want to respect Aboriginal beliefs.

Faced with contradictory statements and no witnesses, the investigator had to conclude there was no evidence to support the complainant's allegation that CSC had tried to collect information about her menses. There could well have been a misunderstanding; her supervisor's somewhat ambiguous response may have exacerbated the situation. It is obvious that any female employee would regard discussion of her menstrual cycle as a private matter and potentially offensive.

Following the Office's investigation (and an internal investigation by the psychiatric centre) the centre issued a standing order advising staff about Aboriginal Offender Programs. The last item, entitled "Special Gifts of Woman Within Aboriginal Spiritual Beliefs" states:

In order to show respect for and work with Aboriginal people, individual involvement and assignment of duties should be on a voluntary basis, where possible.

The centre's executive director confirmed that female staff are not (and never have been) required to advise supervisors or anyone else about their menstrual cycle.

The Commissioner concluded that there was no evidence to substantiate the complaint.

Securing the tax phone line

Occasionally callers do not wait for an improper disclosure but call to alert privacy staff to a potential problem. One case concerned Revenue Canada's automated Tax Information Phone Service (TIPS) which taxpayers can call for basic information about their return or refund.

The complainant, an employer, was concerned that he, and presumably other employers, could call the TIPS line and get employees' tax details because they had the gate-keeping information—employees' social insurance numbers and dates of birth. The employer was prescient; another complainant had his identification stolen and subsequently used to obtain information from TIPS.

The investigator, armed only with a SIN and month and year of birth, called the TIPS number. She was able to confirm that an individual receives quarterly GST refunds and when the refund would be mailed, the individual's RRSP deduction limit for the filing year, and the amount of income tax refund owing.

Clearly the TIPS gate-keeping measures were inadequate and more stringent protections were needed.

Revenue Canada was reluctant to consider changes that would make the system more difficult for taxpayers to operate; TIPS is a convenient and cost-effective way to answer taxpayers' most common questions—it handled more than two million last year.

Revenue Canada rejected the Office's suggestion to assign taxpayers a personal identification number (PIN). It was too impractical and expensive—issuing PINs to every taxpayer would cost over \$4,500,000 in mailing costs alone. Several other options for a third piece of identification were considered and rejected because the identifier was too easy to guess or was not collected in the tax database.

The final proposal resolves the issue. TIPS callers will now be asked to provide their "total income" from line 150 of their tax return. Other callers would be unlikely to have this detail and it would be hard to guess or steal.

Government shares tax, income and social benefit details

Another complaint underscores the need for Canadians to understand that the federal government may disclose their information without their consent in a number of circumstances set out in the *Privacy Act*. While the *Act* controls federal government disclosures of personal information, it does not prevent departments from fulfilling their legal mandates nor shield individuals who are less than frank on their tax returns.

The widow of a Canadian war veteran complained that Revenue Canada disclosed her interest income to Income Security Programs which reduced her Old Age Security Spouse Allowance and Guaranteed Income Supplement. Income Security, in turn, gave the information to Veterans Affairs Canada which cancelled her Foreign War Disability Pension.

The investigator confirmed the allegations were substantially correct. Income Security Programs did not contest the woman's claim. It routinely verifies Old Age Security applicants' income with Revenue Canada, and it had disclosed the interest information to Veterans Affairs. Both departments demonstrated that the disclosures are authorized by law, and so comply with the *Privacy Act* which allows government institutions to disclose personal information if authorized by another law or regulation.

In this case, Revenue Canada's disclosure to Income Security Programs is authorized by section 241 of the *Income Tax Act*, and Income Security Programs' disclosure to Veterans Affairs by section 33 of the *Old Age Security Act*.

The Commissioner considered the complaint not well-founded.

New Customs lookout system "hits" on admin file

A Nova Scotia man discovered why he was being stopped and sent for further questioning each time he crossed the Canada-U.S. border—his name was on the new Customs' Primary Automated Lookout System.

The lookout system includes names of individuals who have violated (or are suspected of violating) one of several statutes that Customs enforces at Canadian borders; for example, immigration, firearms and agriculture laws and regulations. Claiming that Revenue Canada improperly collected the information, he complained to the Commissioner.

Custom's lookout system shares selected information with the Police Information Retrieval System (PIRS), an RCMP data base containing information about events, subjects, vehicles and property. The RCMP system is available to other federal departments. Apparently the complainant had been implicated in an internal Agriculture Canada inquiry into allegations that staff were making personal use of departmental vehicles. Agriculture Canada put this information onto PIRS; whenever Customs officers queried his name at border-crossing points, the system showed a "hit". Believing there was an enforcement lookout for the man, they sent him for "secondary examination".

Since Customs officers were merely responding to information Agriculture Canada put on PIRS, the focus of the investigation shifted to Agriculture. The investigator found that the new Customs lookout system had simply outpaced the programming of PIRS which could no longer distinguish between enforcement information (which Customs needed) and non-enforcement information, which it did not.

To prevent future "hits" on the complainant, Agriculture Canada removed his information from PIRS. It will also stop entering non-enforcement information on the system and remove any that now exists. This should prevent other individuals being confronted with the same problem.

Inquiries

The Office handled 9217 inquiries during the year, an increase of 529 from the previous year.

Although two officers are assigned full-time to answering inquiries, the workload means that virtually all staff answer the public's questions. Staff provide details on the *Privacy Act*, the complaints process, basic information on privacy issues not in the Office's jurisdiction, and—where necessary—referrals to other government agencies and the private sector. Inquiries staff also do a preliminary assessment to determine whether the problem is within the Commissioner's jurisdiction and can be investigated. If so, they act as first level of intake for a complaint.

The Visa Gold Card application

More than 100 calls were prompted by a new Royal Bank Visa Gold application asking clients to allow the bank to use their Social Insurance Numbers (SINs) for a wide range of other services. The *Income Tax Act* requires customers to provide their SINs to financial institutions for interest statements. However, it also forbids financial institutions from using SINs for other purposes without the customer's consent. Unfortunately Royal Bank's request for consent is so broad that it constitutes a virtual waiver of the protection set out in the *Income Tax Act*. It reads:

If I have ever given you my social insurance number, you may treat it as Information and use it as an aid to identify me with credit bureaux and other parties.

Even if I am no longer your client or this Agreement terminates, you may keep Information in your records and use it for the purpose noted above.

The Commissioner discussed these blanket waivers in a recent appearance before the Senate Banking Committee which reviews the financial industry. Privacy of customers' records is one of the issues the committee is examining, following changes to legislation governing banks, trust and insurance companies.

Putting personal data on the highway

The hype (and confusion) surrounding the information highway led to many callers wanting the Office's advice on how better to protect themselves in view of the lack of legal protection in the private sector. Staff can only offer general advice on transmitting any personal data by interactive networks:

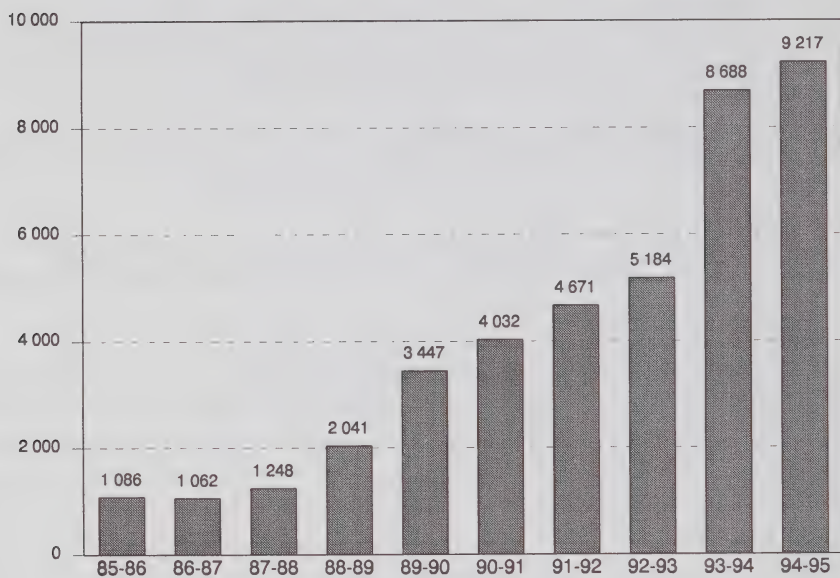
- assume the system is not secure unless the carrier can prove to the contrary—don't transmit any personal information you're not prepared to have anyone know;
- don't give out bank card numbers and financial information unless the system encrypts the information;
- ask the operators of user groups how they store and use the personal details you supply to identify yourself as a legitimate user; are they secure?

There were almost a 1000 calls about private companies posting employees' overtime payments, SINs, home addresses and other personal information on bulletin boards. This may be insensitive but it is not against any law (with the possible exception of Quebec which has private sector privacy protection). Employees are advised to try to resolve the matter with human resources staff or with their union.

Several callers complained that they were unable to access their medical or psychological files; these were referred to the Royal College of Physicians and Surgeons.

The table illustrates the growth in inquiries handled.

Inquiries 1985-95



Top Ten Departments by Complaints Received

Institution	TOTAL	Grounds		
		Access	Time Limits	Privacy
Correctional Service Canada	331	148	136	47
National Defence	274	62	164	48
Revenue Canada	237	48	147	42
Royal Canadian Mounted Police	154	76	44	33
Human Resources Development Canada	150	42	52	56
Citizenship and Immigration Canada	129	26	90	13
Canadian Security Intelligence Service	101	95	4	2
Canada Post Corporation	97	52	20	25
Immigration and Refugee Board	34	15	16	3
National Parole Board	26	16	9	1
OTHER	250	120	47	80
	TOTAL	1783	704	350

Completed Complaints by Grounds and Results

Grounds		Disposition					TOTAL
		Well-founded	Well-founded; Resolved	Not Well-founded	Resolved	Discontinued	
Access		17	105	329	0	21	472
	Access	13	100	306	0	20	439
	Correction/Notation	4	5	22	0	0	31
	Inappropriate Fees	0	0	0	0	0	0
	Index	0	0	1	0	0	1
	Language	0	0	0	0	1	1
Privacy		58	14	141	26	17	256
	Collection	4	4	40	26	8	82
	Retention & Disposal	13	0	9	0	0	22
	Use & Disclosure	41	10	92	0	9	152
Time Limits		394	6	176	0	3	579
	Correction/Time Limits	21	0	1	0	0	22
	Time Limits	354	6	102	0	3	465
	Extension Notice	20	0	72	0	0	92
TOTAL		469	125	646	26	41	1307

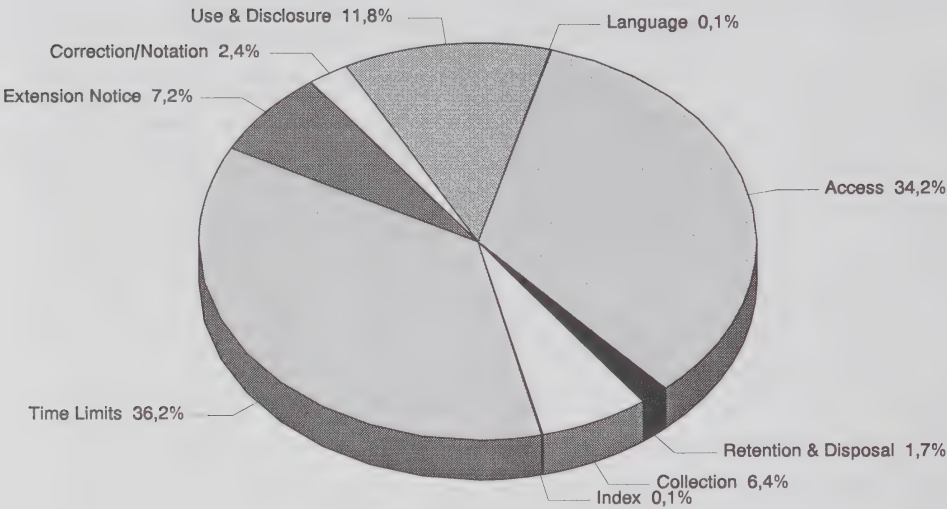
Completed Complaints by Department and Result

Department	Total	Well-founded	Well-founded; Resolved	Not well founded	Discontinued	Resolved
Agriculture and Agri-Food Canada	39	20	5	12	2	0
Bank of Canada	1	0	0	1	0	0
Canada Labour Relations Board	7	2	2	3	0	0
Canada Mortgage and Housing Corporation	2	0	0	2	0	0
Canada Ports Corporation	2	0	1	1	0	0
Canada Post Corporation	99	9	14	67	9	0
Canadian Human Rights Commission	4	0	2	2	0	0
Canadian Security Intelligence Service	51	0	0	51	0	0
Canadian Space Agency	3	1	0	2	0	0
Citizenship and Immigration Canada	45	31	1	7	6	0
Communications Canada, Department of	1	0	1	0	0	0
Correctional Investigator Canada	1	0	0	1	0	0
Correctional Service Canada	195	72	12	101	10	0
Elections Canada	2	0	0	2	0	0
Employment and Immigration Canada	89	43	7	38	1	0
Energy, Mines and Resources	1	0	0	1	0	0
Environment Canada	8	5	0	3	0	0
Farm Credit Corporation Canada	1	0	0	1	0	0
Finance Canada, Department of	1	0	0	1	0	0
Fisheries and Oceans	5	5	0	0	0	0
Foreign Affairs and International Trade Canada	1	0	0	1	0	0
Health Canada	31	7	7	16	1	0
Human Resources Development Canada	51	20	4	21	6	0
Immigration and Refugee Board	39	6	13	20	0	0
Indian and Northern Affairs Canada	44	21	1	22	0	0
Industry Canada	5	1	0	4	0	0

Completed Complaints by Department and Result

Department	Total	Well-founded	Well-founded; Resolved	Not well founded	Discontinued	Resolved
Justice Canada, Department of	12	5	4	3	0	0
National Archives of Canada	14	0	1	12	1	0
National Defence	162	88	13	60	1	0
National Parole Board	26	3	6	16	1	0
Privy Council Office	7	3	1	3	0	0
Public Service Commission of Canada	6	2	3	1	0	0
Public Works and Government Services Canada	1	0	0	0	1	0
Revenue Canada	189	116	12	60	1	0
Royal Canadian Mint	3	0	0	3	0	0
Royal Canadian Mounted Police	100	5	11	83	1	0
RCMP Public Complaints Commission	5	0	0	5	0	0
Secretary of State	4	1	1	2	0	0
Security Intelligence Review Board	1	0	0	1	0	0
Solicitor General Canada	4	0	0	4	0	0
Statistics Canada	27	1	0	0	0	26
Transport Canada	10	0	3	7	0	0
Transportation Safety Board	5	0	0	5	0	0
Treasury Board of Canada Secretariat	2	2	0	0	0	0
Veterans Affairs Canada	1	0	0	1	0	0
TOTAL	1307	469	125	646	41	26

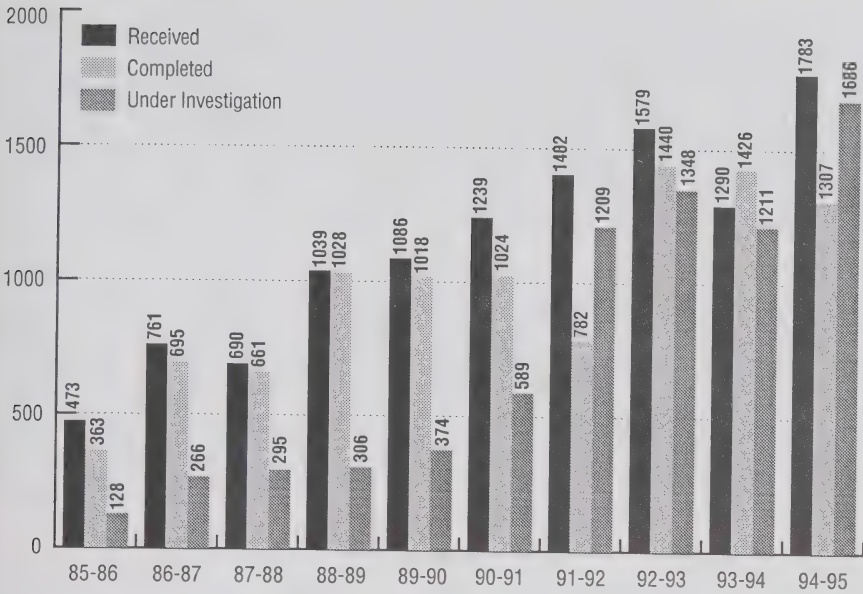
Complaints Completed by Grounds



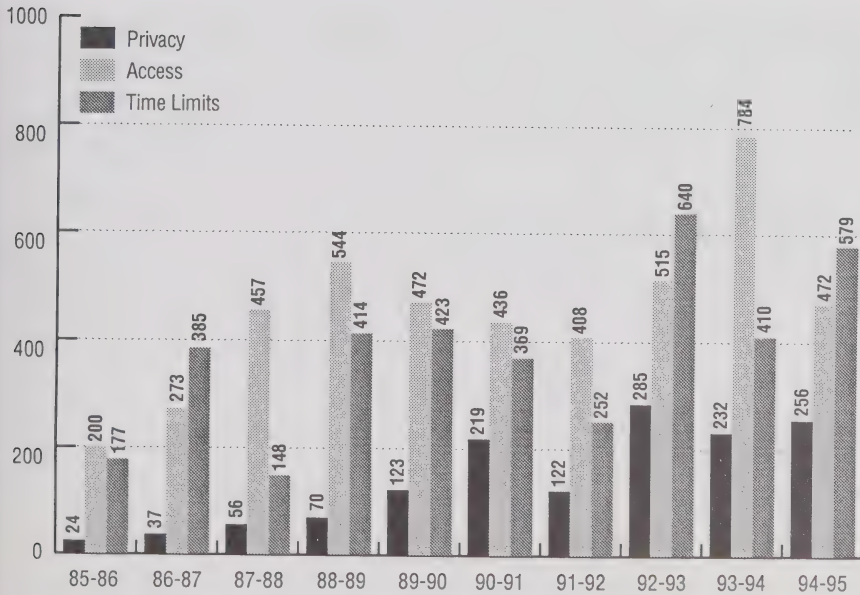
Origin of Completed Complaints

Newfoundland	8
Prince Edward Island	3
Nova Scotia	36
New Brunswick	25
Quebec	112
National Capital Region Quebec	12
National Capital Region Ontario	240
Ontario	438
Manitoba	35
Saskatchewan	63
Alberta	76
British Columbia	233
Northwest Territories	3
Yukon	1
Outside Canada	22
TOTAL	1307

Completed Complaints 1985-95



Completed Complaints and Grounds 1985-95



Monitoring Compliance

The impact of federal government restructuring took affect with a vengeance this year. Following on the heels of the June 1993 re-organization (reported last year) came Program Review—a fundamental re-examination of every federal program and activity (including more than 400 agencies, boards and commissions), then the February 1995 budget. The result was closure of 73 agencies, streamlining 47 others and announced staff cuts of 45,000 employees—20,000 by the summer of 1996.

Departmental staff who process personal information applications did not escape the cuts. But the workload had not diminished; it is simply spread among those who are left. The effect was predictable. Unable to meet the statutory deadline of 30 days to reply, departmental staff saw their application backlog mounting and a steady increase in delay complaints to the Privacy Commissioner. These delays are a factor in the Office's mounting complaint load.

The scale of the changes left departments scrambling to redesign or integrate many informatics systems, move client and employee files to new homes, and decide how to store or dispose of personal records that no longer had a home.

Reorganization also made following up earlier audits much more complex; recommendations that applied to old work units now had to be explained to managers who had inherited the programs (or lost them in the shuffle). For example, the Office of the Comptroller General, audited in 1992, merged with the Treasury Board Secretariat. TB and privacy staff had difficulty tracing files, and decisions concerning personal information that had been transferred.

Moving to a portfolio system

The Office has had to reduce its dependence on routine audits to assess government compliance—the workload is simply beyond the four staff available for the task. Staff are now assigned as portfolio leaders to develop an understanding of the agencies' business and programs and to operate as a first line contact for government staff seeking advice. This more active stance should help prevent privacy problems in a department and even develop solutions government-wide.

With the new portfolio system in place, the Commissioner wrote to all deputy heads outlining the Office's new approach and offering its services. The offer was taken up with a vengeance. Portfolio leaders met and briefed privacy coordinators representing more than 80 federal agencies, as well as holding information sessions for more than 400 employees, senior executives, technical experts, correctional staff and representatives of a private company working on a major re-engineering project.

Responding to the requests proved a tall order for staff who received a constant stream of calls to explain the *Act* and clarify policy and its application in various situations.

Managers sometimes show little interest in privacy until they discover its impact on staff relations, informatics systems design and holdings, client and employee personal information, and information sharing projects with other departments, governments or the private sector. Once they understand the implications, they are only too glad to seek advice and forestall problems.

Two examples dealt with during the year illustrate the advantage of examining issues government-wide; disposing of surplus (particularly computer) assets, and sharing personal information with other agencies and governments.

Disposing of surplus assets

The saga of sloppy disposal of surplus assets continues. The 1992-93 report told of a former office employee buying a surplus file cabinet and finding hundreds of file cards documenting individuals' lab tests. Lightning struck again this year. The office bought a safe from a Crown Assets Distribution Centre and discovered several RCMP documents, including secret contingency plans and performance appraisals of senior RCMP members.

In October, a man found used computer diskettes containing confidential information about a GST registrants in a file cabinet bought at a government surplus sale. These are just the federal government incidents in a litany of disclosures involving discarded cabinets, old computers and second-hand diskettes reported in the media.

Pinning down responsibility for ensuring surplus cabinets, computers and diskettes are empty has not been easy. There has been a good deal of buck-passing. Getting concrete action to solve the problem has demanded the cooperation of Treasury Board, Crown Assets, the RCMP and departments themselves. The Office has pressed the major players steadily and now has an agreement.

Who does what

But first, here is how the responsibilities break down. Crown Assets is usually (but not always) the final gate before surplus material goes to market. However, it does not have enough staff to verify that all surplus goods have been emptied of sensitive information. That responsibility remains with the original owners. Frequently Crown Assets does not even see surplus desks or filing cabinets, serving simply as a clearing house to direct interested buyers to departments with available material.

The RCMP Security Engineering Section opens surplus safes, restores the combination to the factory setting and returns them to Crown Assets, which assumes they are clean and makes no further check.

In addition, six departments are participating in a pilot project to dispose of their own surplus through trade-ins and interdepartmental transfers, without notifying Crown Assets.

Finally, obsolete computers are sent to the Computers for Schools Program run by Industry Canada. Last year the program reported that about 95 per cent of all donated computers contained data and programs, despite government directives to clean computer disks. This year the news is better; 35 to 45 per cent of all donated federal computers were clean. Progress indeed but plenty of room for improvement—the remaining 55 to 65 per cent still represents a lot of government data.

Now the agreement:

- Crown Assets will amend the form on which federal institutions list sale items to require they certify the assets have been cleared of any sensitive or classified material. This is to be done for the July 1995 printing.

- Crown Assets will inform client departments about the change in flyers or newsletters, flag the changes to all distribution centres across Canada and amend its Customer Manual.

- Once the pilot electronic bulletin board system for government materiel managers is operational, it will include a permanent message reminding anyone trading or exchanging surplus assets to ensure they have been emptied of any sensitive information.

■ The RCMP has sent bulletins to all departments describing an RCMP-approved utility which wipes all data from computers' hard drives. The RCMP can only keep reminding staff that the hard drives of old computers should be completely erased.

■ Treasury Board Secretariat will write to all assistant deputy ministers asking them to ensure their departments have procedures in place to prevent any unauthorized disclosures of classified or designated information, including improper disclosures through the disposal of surplus assets.

■ Both the Board and Crown Assets agreed to publicize the issue through publications distributed to federal government material managers.

The agreement will not necessarily spell the end of these careless disclosures. However, it should at least ensure that government agencies put the necessary safeguards in place and alert their employees to the dangers of improperly disposing of surplus assets.

The federal government now needs to make similar efforts to ensure data cannot be retrieved from computer hard drives, tapes and diskettes which are damaged beyond repair. Sending hard disks to the local dump is not the answer; anyone with computer knowledge can extract some of the information. These media must also be purged of data or destroyed in such a way that they information cannot be retrieved.

Sharing personal information— agreements and "arrangements"

This year marked the Office's first attempt to maximize its use of its minimal audit resources by taking a "systemic" approach—reviewing one aspect of government handling of personal information

across all agencies. The issue is sharing client information with other programs or organizations.

Knowing what personal information government shares, how, and with whom are fundamental to both individual citizens' privacy rights and to the Commissioner's effective oversight. Although the *Privacy Act* prevents government from using personal information for purposes other than for which it was collected (section 7), it does set out a number of lawful disclosures (section 8).

One of these allows a federal government agency to enter "an agreement or arrangement" to share information with the another government (or an organization of governments) to administer a law or carry out a lawful investigation.

Treasury Board has published guidelines on information sharing agreements but not on what constitutes "an arrangement". And government departments are not required to notify the Privacy Commissioner when entering an agreement—as they are when conducting a data match.

Early in 1995, the Office surveyed all 110 institutions subject to the *Privacy Act* to determine how much formal and informal sharing and data matching of personal information was taking place. The four-part questionnaire asked respondents to list all data matches and sharing agreements or arrangements both inside and outside the organization—93 responded.

The study revealed that 47 do not share personal data inside or outside the organization, two share internally, 17 share with outside organizations but not internally, 27 share both inside and outside, and 18 reported data matches.

The second phase of the study will verify the data and examine selected agreements and arrangements. The Office will also develop guidelines and be better prepared to advise federal institutions on sharing information next year.

Data matching

Data matching is the technical process governments often use to share information. Essentially data matching compares information about individuals from different sources to make decisions about their benefits or services. Once conducted by sharing computer tapes, increasingly the trend is to allow other users—either other parts of the organization or other governments—direct access to on line data bases.

A 1989 government policy requires government agencies to conduct detailed assessments of proposed data matches, and to notify the Privacy Commissioner. However, existing matches continue unreported; there is no mechanism to allow the Commissioner to gauge the scope of federal government data matching.

The Office reviews data match proposals against the following criteria:

- the information cannot be obtained by other methods;
- the collection relates directly to an operating program of the federal department;
- direct collection would be counterproductive;
- the information will be accurate, up-to-date and complete, and
- the benefits of the match clearly outweighs any subsequent invasion of privacy.

Three Human Resources programs

Three recent cases at Human Resources Development Canada (HRD) illustrate how personal information is shared among federal, provincial and municipal governments to control abuse of federal unemployment insurance and provincial and municipal social benefit programs.

Unemployment Insurance with Canada Pension Plan: HRD conducted a feasibility study to try to estimate losses from payments to individuals claiming both unemployment insurance and Canada Pension Plan disability benefits. (Anyone receiving CPP disability benefits is unable to work and therefore not entitled to unemployment insurance.) The study matched lists of those receiving benefits from both programs and estimated losses of more than \$20 million a year.

Following the study, HRD determined it was both feasible and cost effective to match the two data bases regularly, and submitted its data match assessment to the Privacy Commissioner. It was clear from the assessment and discussions with HRD staff that the benefits from the data match clearly outweighed any invasion of privacy. Clients sign a consent to verify the information on the application forms.

Workers' Compensation with Unemployment Insurance: A second HRD study targeted individuals who were receiving benefits from both the Ontario Workers' Compensation Board and the Unemployment Insurance Program. This study also identified potential losses of over \$20 million a year from overpayments. Following its assessment, Office staff concluded that the benefits clearly outweighed the invasion of privacy.

The third case was not a data match but changes an existing information sharing procedure. Although not required to, HRD chose to consult the Office to forestall any problems.

Ontario social service with Unemployment Insurance: The change allows municipal social services staff direct access by dedicated computer terminals to limited personal data on HRD's unemployment insurance data base. This allows them to confirm that an applicant for social service benefits has applied for unemployment insurance. Provincial social assistance programs provide benefits to the needy to bridge the mandatory three-week waiting period for UI (and possibly two to three weeks to process the application). Applicants must sign an undertaking to repay any overlapping UI payments to social services.

Allowing social services staff direct access frees HRD staff from responding to numerous calls from social service staff, saves social services staff time and spares the applicant from travelling between two offices.

Notifying the Commissioner

Reviewing public interest disclosures

Overall, the number of disclosure notices rose slightly; 56 compared to 48 last year. Some departments are beginning to use the disclosure provisions systematically. One of these is Correctional Service Canada which was responsible for 22 of the 56 disclosures reviewed this year.

The vast majority of CSC's disclosures resulted from media requests under the *Access to Information Act* for internal reports on inmate escapes or violent incidents in penitentiaries. These reports usually contain personal information about inmates, victims and staff, and often discuss the factors determining the penitentiary in which the inmate is confined and the conditions of parole.

Mounting public concern about sentencing and parole, particularly of dangerous offenders, is pressuring CSC to disclose all the factors it and the National Parole Board weigh in making these decisions. And whenever an incident occurs (for example, an inmate committing murder while on day parole), CSC considers that the public has a right to information which might have been a factor in the incident. Often this leads to disclosing a lot of sensitive personal information. Occasionally, in an effort to be open and accountable, the institution reaches too far.

However, one lesson learned long ago is that privacy exemptions cannot be self-serving. CSC and NPB must not—and do not—exempt information that is critical of its or its employees' decisions or actions under the guise of protecting their privacy.

The disclosure provisions require a delicate balancing act. "Public interest" is more than public curiosity. The institution must demonstrate how this interest outweighs an individuals' privacy rights. Even justified disclosures demand careful examination.

Investigating incidents

Portfolio managers also investigated ten incidents leading to possible loss, theft or improper disclosure of personal information.

Regular readers may note that most of past years' incidents appear to originate with a handful of institutions: Correctional Services Canada, the National Parole Board, Veterans Affairs Canada and Revenue Canada. This year is no exception.

This does not mean other departments' information management practices are so superior that they never lose, compromise or have personal information stolen. In fact, these organizations are among the few which take seriously their responsibility to advise the Commissioner that personal information may have been compromised. There is a positive side to notifying the Commissioner; it gives program staff an opportunity to enlist the Office's help in correcting—and ultimately preventing—a recurrence.

CSC accounted for six of the 10 incident investigations opened by this Office in the year under review. All were caused by improperly handled personal information.

Woman's name & address to inmate

In one case, CSC wrote to a woman who was seeking information about a family member. Staff mistakenly put the letter in an envelope addressed to an inmate who is serving sentence for violent crimes against women in a penitentiary near the woman's home.

Although the inmate will not be released for several years, privacy staff were concerned that the disclosure could seriously jeopardize the woman's safety.

CSC readily admitted its mistake. At the Office's urging, a CSC employee visited the woman to explain what had happened and to advise her about the situation. Apparently she was not unduly concerned and did not want CSC to take any further action. CSC will change its mailing procedures to prevent this happening again.

SINs on envelopes

One incident led to a number of complaints; Revenue Canada mailed a special tax guide to more than 700,000 taxpayers with their social insurance numbers (SIN) printed on the mailing label.

The Office learned of the problem first from a journalist, then from several callers who received the package. The faulty labels had been fixed to special guides sent to taxpayers who reported rental income on last year's income tax returns, and to northern residents. The SIN (which is personal information) would have been visible to anyone handling the guide prior to delivery. Revenue Canada does not require the SIN to be displayed; the guides would reach the intended recipients without the SIN on the wrapper label.

The investigators determined that three separate processing failures caused the disclosure. First, staff should have removed the SIN from computer tapes used to prepare the mailing list before sending it to the printer. Second, Revenue Canada did not specify precisely what information was to appear on the labels. Third, staff should have checked label samples before allowing the mailing.

Revenue Canada recognizes its obligation to keep the SIN confidential. The deputy minister took a personal interest and the department quickly took steps to prevent a recurrence.

Audits and Follow-ups

This year staff completed two major audits at Immigration and Consumer and Corporate Affairs (both of which have since been incorporated into new departments), as well as smaller audits of the Canada Council and both the Pacific and Atlantic Pilotage Authorities. This finishes work at the four pilotage authorities.

Consumer and Corporate Affairs

The Office has wrapped up the one remaining issue from its 1993-94 audit of Consumer and Corporate Affairs Canada (CCA—now Industry Canada). In dispute were some of the contents of public records kept by the Superintendent of Bankruptcy.

The *Bankruptcy and Insolvency Act (BAA)* requires the Superintendent to maintain a public registry of all insolvency proceedings—bankruptcy, proposal and receivership. In addition, some branch employees now act as Official Receivers; in effect the branch becomes the equivalent of a court of record. This means that certain documents dealing with these cases are considered public in the same manner as those filed in a court.

Auditors reviewed a sampling of bankruptcy files and found that some contained a wide range of personal information, not only about the person declaring bankruptcy but also about family members and creditors. For example, some files included details about the person's use of alcohol or addiction to gambling; others, if the creditor was an individual, his or her home address, telephone number and Social Insurance Number. CCA staff could not define which elements of personal information were needed for the public register or records that are open for public inspection.

Establishing what constitutes a public record is critical since provisions of the *Privacy Act* dealing with an institution's use and disclosure of personal information (sections 7 and 8), do not apply to any "publicly available" information.

The Superintendent examined the files and established a precise definition of which elements of personal information constitute the public register, and which documents are open for public inspection. The remaining personal details would have the full protection of the *Privacy Act*.

The Commissioner accepted the new definition and recommended the Superintendent communicate them to all Bankruptcy staff and amend procedures to ensure that the remaining personal information in the files is protected.

Immigration

Privacy staff also completed auditing the Immigration Group of Employment and Immigration Canada during 1993-1994. However, they could not report the results and many outstanding issues owing to the upheaval surrounding its reorganization and integration into the new department of Citizenship and Immigration.

The mandate of the audit was to examine the department's handling of employees' and clients' personal information, including at a number of the department's approximately 900 regional offices. Immigration maintains personal information in 26 information banks on the 6.7 million individuals who have come to Canada since 1946.

To process and store this information, the department has two major informatics systems, the Field Operations Support System (FOSS) and the Computerized Immigration Processing System (CIPS), as well as many sub-systems. The CIPS data is accessible in Canadian Visa Offices around the world. The department's current reorganization should have a significant impact on management of its electronic records and files and

Office staff are approached regularly for advice on the privacy implications.

Our auditors noted short-comings in some key areas, but given the "re-engineering" process, confined recommendations to the informatics systems. These recommendations include:

- incorporating a privacy alert in the software used to manage and transmit personal information between buildings;
- incorporating commands in the software used to extract and print personal information from databases which will add a privacy statement to each printed document informing users about the requirements of the *Privacy Act*;
- conducting a threat and risk assessment for all informatics systems and communications networks;
- arranging for SEIT (RCMP) inspection of informatics systems to assess the security status of these installations;
- establishing written criteria for granting access rights to the personal information contained in the informatics systems;
- incorporating an audit trail into informatics installations to allow managers to determine who has access to what personal information and for what purpose;
- adding an encryption feature to all portable computers to protect the personal information they contain in case of lost or theft.

The department invited the portfolio leader to provide advice on privacy issues to senior managers and staff during meetings on the re-engineering project. Next year's report will document the progress.

Pacific and Atlantic Pilotage Authorities

These two pilotage authorities provide pilots to guide ocean-going vessels in Canadian waters. (The Laurentian and Great Lakes authorities were audited in 1991.) Most pilots are hired on contract and the authorities collect and manage very little personal information. Their files include information about pilots' certificates, medical information, and reports about any accidents in which pilots may have been involved. Files may also contain information on ship crew misconduct.

Auditors recommended adding and amending bank descriptions in Info Source, improving notification to individuals about how the authorities' use the personal information, and revising contracting-out procedures to address privacy concerns. Both Authorities have agreed to institute corrective measures.

Canada Council

The Canada Council provides funds and grants to artists, art professionals and artistic organizations to foster and promote the arts in Canada. It also acts as Secretariat for the Canadian Commission for UNESCO. The council creates an average of 15-20,000 files each year, almost all of which contain personal information. The holdings include basic data on artists, assessors and juries, and records from competitions and grant applications, including comments by assessors and juries on individual candidates. There is also a complete range of employee data.

The audit was re-scheduled from the previous year at the council's request. Nevertheless, the council has undergone an extensive re-organization and down-sizing since the audit was conducted.

The most significant recommendations concern the need for written policies and procedures on managing personal information and for staff training about the requirements of the *Privacy Act*.

Despite recent council efforts, staff are still not conversant with the concept of "personal information"; this deficiency is reflected in the protection council staff give personal information.

The Commissioner made several recommendations concerning the council's collection, use, disclosure and protection of personal information. The council should

- develop a written policy and procedures on managing personal information and distribute them to staff and to external assessors who evaluate grant applications;
- review its collection procedures and forms and add a privacy rights statement to all those that do not yet have one;
- obtain explicit consent from individuals for using their names and other personal details for mailing lists;
- develop a written security policy and review practices which could compromise the confidentiality of its personal information holdings;
- have the RCMP Systems Audit and Evaluation Investigation Team assess the security of the computer facilities;
- include privacy clauses in future contracts with outside organizations, stipulating that any personal information collected or generated is the exclusive property of the council;
- issue specific instructions on secure disposal of computer equipment and storage media before discarding or selling;
- prevent staff of other organizations with whom it shares facilities from accessing personal information in data bases or storage media;

- instruct staff on the use of laptop computers outside council premises when the hard disk contains personal information, and equip each laptop with a security device, and

- complete an index of all personal information holdings and mailing lists and review the *Info Source* listing to ensure their accuracy.

Follow-ups

This year staff continued following up earlier audits to determine whether the organizations had implemented the Commissioner's recommendations. Portfolio leaders reviewed audits of 9 institutions and found 37 of 39 recommendations (95 per cent) had been completely implemented, a significantly higher proportion than last year's 77 per cent. One recommendation had been partially implemented. One other finding is no longer applicable.

Staff reviewed Telefilm Canada, Transportation Safety Board of Canada, Canadian International Trade Tribunal, Office of the Chief Electoral Officer, Canada Deposit Insurance Corporation, Veterans Affairs Canada, Veterans Appeal Board, Bureau of Pensions Advocates and the Office of the Comptroller General.

The organizations have responded to all recommendations about increasing staff awareness. One had also developed a policy concerning the secure transmission of personal information by fax. Another dedicated a new printer to its human resources unit, placing it in a secure area to prevent other staff from seeing personnel information.

Approximately half of the organizations reviewed need to change their retention and disposal practices to comply with the *Privacy Act*. All but one of these have submitted retention and disposal schedules for National Archives approval. One department conducts random spot checks to ensure that no sensitive material is sent for recycling.

Auditors often find that the information bank listings in *Info Source* are inadequate or non-existent. This year was no exception. Recommendations were made to all organizations except the Transportation Safety Board to edit, add or amend their listings. The organizations have complied.

Keeping *Info Source* listings accurate and up-to-date is key to individuals exercising their access and correction rights. Incomplete or inaccurate listings mean the government is not meeting a fundamental obligation under the *Privacy Act*—to spell out what information it collects and how the data is used and disclosed.

Office of the Chief Electoral Officer

In November 1994, the Office completed follow-up of its 1992 audit of the Office of the Chief Electoral Officer (Elections Canada). Elections Canada organizes federal elections and referenda and compiles the federal electors list. Elections Canada has acted on 10 of the 11 recommendations contained in the report, including both administrative changes and amendments to the *Canada Elections Act*.

The one outstanding recommendation concerns RCMP review of Elections Canada's EDP system security. Although it has put additional EDP controls in place, its systems have yet to be reviewed by the Security Evaluation and Inspection Team to ensure they conform to accepted security practices. Elections Canada assured the Commissioner that the review would occur in the near future. System security is critical given Elections Canada's project to develop a permanent voters' list.

The permanent voters' register

The idea of a permanent voters register was first discussed in 1988. It would replace the costly and time-consuming door-to-door enumeration, problems exacerbated by urban Canadians' growing concern with providing information to strangers at the door.

Given the obvious privacy concerns with a permanent electronic register, the Commissioner accepted Elections Canada's invitation to participate in a working group studying the feasibility of a register to be used in all federal, provincial and municipal elections. Privacy staff would provide advice on such privacy pitfalls as whether the information would be collected from other electronic databases—and how, who would have access to the register, its security and the accuracy and completeness of the data.

Corporate Management

The Information and Privacy Commissioners share premises and administrative services for economy and efficiency but operate independently under their separate statutory authorities. Corporate Management provides centralized administrative services to avoid duplicating effort and to realize cost savings to the government. The services include finance, personnel, information technology advice and support, and general administration (including records management, security, procurement, library, reception and management services).

The Branch is a frugal operation with 14 staff (who perform a variety of tasks) and a budget accounting for just 15 per cent of the overall OIPC budget. While the Branch will continue to improve productivity, it is at that precarious line between being lean and what the Privacy Commissioner has described as "fiscal anorexia".

Resource information

The Offices' combined budget for the 1994-95 fiscal year was \$6,696,000, a decrease of \$123,000 over 1993-94. Actual expenditures for the 1994-95 period were \$6,522,356 of which, personnel costs of \$5,300,465 and professional and special services expenditures of \$584,559 accounted for more than 90 per cent of all expenditures. The remaining \$637,332 covered all other expenditures including postage, telecommunications service, office equipment and supplies.

Expenditure details are reflected in figure 1 (resources by organization/activity) and figure 2, (details by object of expenditure).

Figure 1: 1994-95 Resources by Organization/Activity

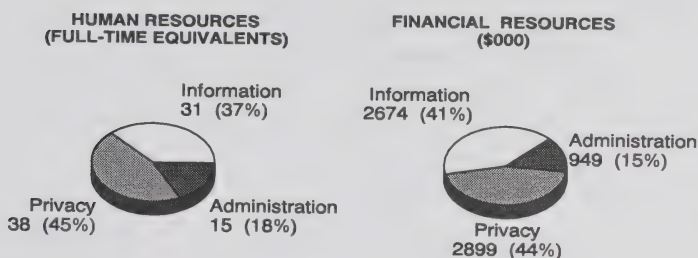
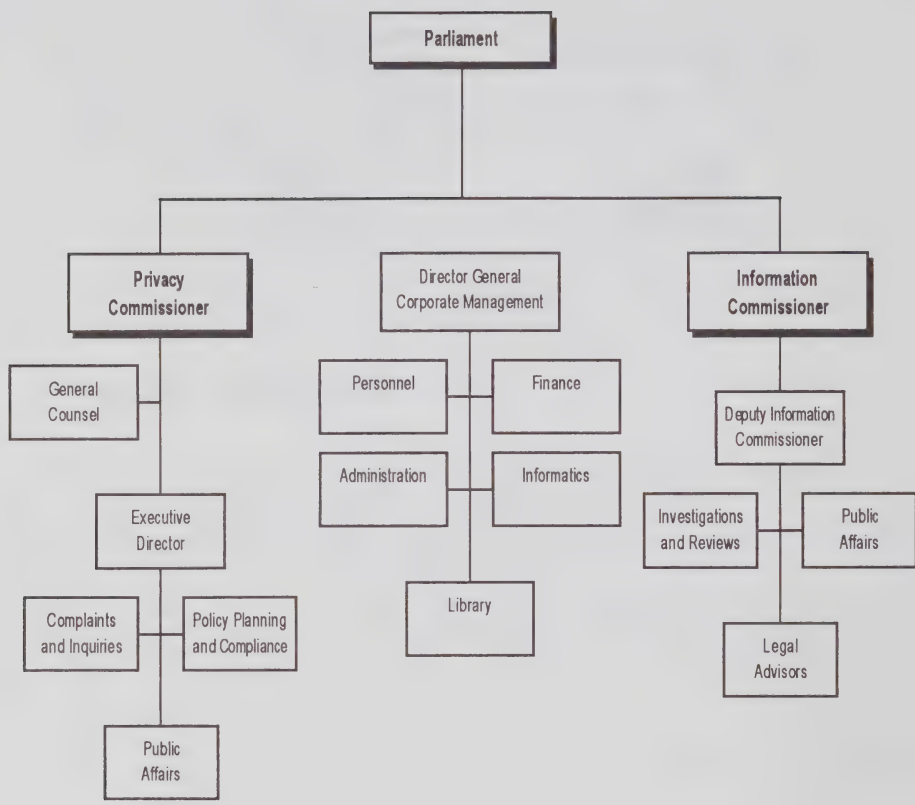


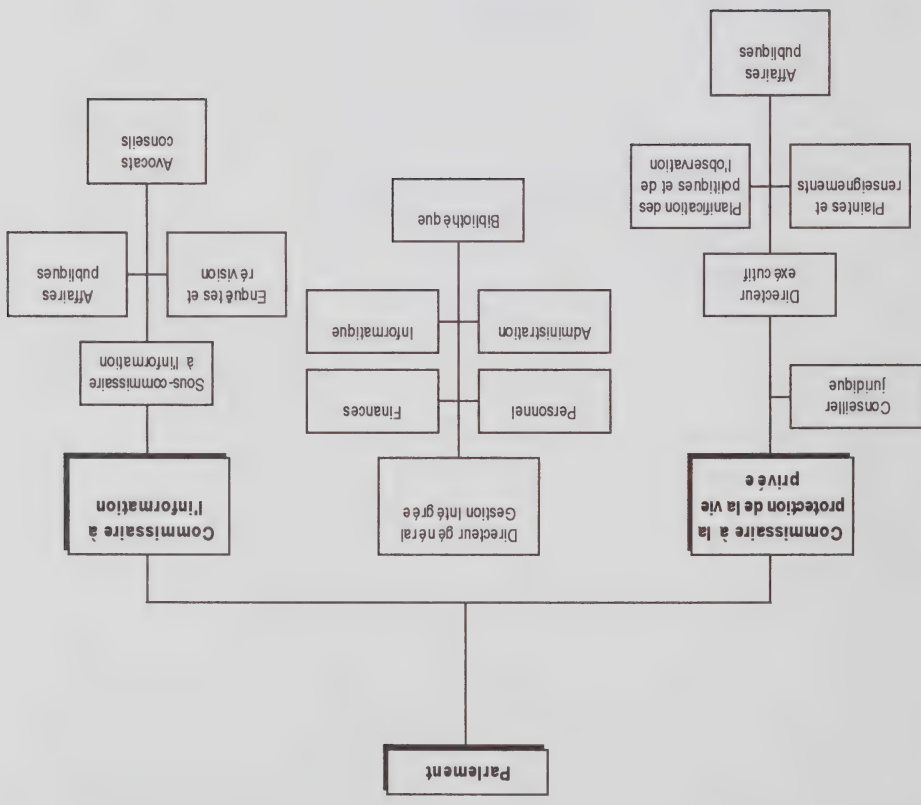
Figure 2: Details by Object of Expenditure

	Information	Privacy	Corporate Management	Total
Salaries	1,820,595	2,252,850	587,020	4,660,465
Employee Benefit Plan Contributions	255,000	299,000	86,000	640,000
Transportation and Communication	58,653	78,470	106,272	243,395
Information	44,182	74,436	2,754	121,372
Professional and Special Services	345,823	134,371	104,365	584,559
Rentals	25,323	589	12,883	38,795
Purchased Repair and Maintenance	21,118	9,559	5,323	36,000
Utilities, Materials And Supplies	25,326	21,195	31,494	78,015
Acquisition of Machinery and Equipment	75,516	27,260	12,906	115,682
Other Payments	2,871	845	357	4,073
Total	2,674,407	2,898,575	949,374	6,522,356

Expenditure Figures do not incorporate final year-end adjustments reflected in the Offices' 1994-95 Public Accounts.

Organization Chart





La ventilation des dépenses est illustrée au Tableau 1 (Ressources par organisation/activité) et au Tableau 2 (Ventilation par type de

dépense).

Tableau 1 : Ressources utilisées en 1994-1995, par organisation/activité

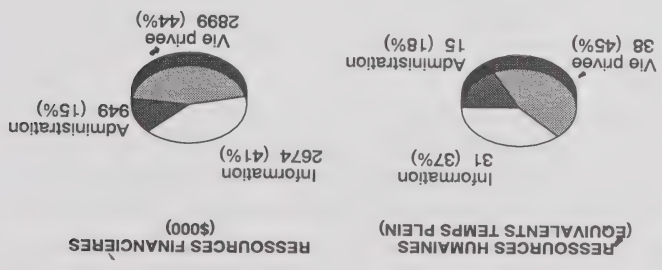


Tableau 2 : Ventilation par type de dépense

	Information	Vie privée	Gestion intégrée	Total
Salaires	1 820 595	2 252 850	587 020	4 660 465
Contributions aux régimes d'avantages sociaux du personnel	255 000	299 000	86 000	640 000
Transports et communications	58 653	78 470	106 272	243 395
Information	44 182	74 436	2 754	121 372
Services professionnels et spéciaux	345 823	134 371	104 365	584 559
Locations	25 323	589	12 883	38 795
Achat de services de réparation et d'entretien	21 118	9 599	5 323	36 000
Services publics, fournitures	25 326	21 195	31 494	78 015
Acquisition de machines et d'équipement	75 516	27 260	12 906	115 682
Autres dépenses	2 871	845	357	4 073
Total	2 674 407	2 898 575	949 374	6 522 356

* Les dépenses n'incluent pas les ajustements de fin d'année reflétés dans la section des Comptes publics 1994-1995 sur les Commissariats.

Gestion intégrée

Par souci d'économie et d'efficience, le Commissariat à l'information et le Commissariat à la protection de la vie privée partagent des locaux et des services administratifs, mais ils fonctionnent indépendamment en vertu des deux lois habilitant leurs opérations. La Gestion intégrée assure les services administratifs centralisés pour les deux commissariats, afin d'éviter le double emploi et de réduire les coûts. Les services dispensés comprennent les finances, le personnel, les conseils et le soutien technologique, ainsi que l'administration générale (gestion des documents, sécurité, achats, bibliothèque, réception et services de gestion).

La Direction est efficiente, avec un effectif de 14 personnes chargées de tâches variées et un budget correspondant à 15 p. 100 seulement du budget total des deux Commissariats. Elle va continuer à améliorer sa productivité, mais elle est actuellement à la limite de ce que le Commissaire à la protection de la vie privée qualifie d'"anorexie financière".

Description des ressources

Le budget combiné des deux Commissariats pour l'exercice financier 1994-1995 était de 6 696 000 \$, en baisse de 123 000 \$ par rapport à 1993-1994. Les dépenses réelles pour la période envisagée se sont élevées à 6 522 356 \$, dont 5 300 465 \$ pour la gestion du personnel et 584 559 \$ pour les services professionnels et spéciaux, ce qui totalise plus de 90 p. 100 de toutes les dépenses. Le reste, soit 637 332 \$, couvre tous les autres frais, c'est-à-dire la poste, le téléphone, le matériel de bureau et les fournitures.

Liste électorale permanente

C'est en 1988 qu'on a commencé à parler d'une liste électorale permanente qui permettrait d'éliminer le processus coûteux et laborieux d'énumération porte-à-porte des électeurs, de plus en plus difficile parce que les citoyens canadiens sont de plus en plus réticents à donner des renseignements aux étrangers qui frappent à leur porte.

Comme une liste électorale électronique permanente soulève de sérieuses questions au chapitre de la protection de la vie privée, le Commissaire a accepté l'invitation d'Élections Canada de participer aux travaux du groupe chargé d'étudier la possibilité d'une liste électorale susceptible d'être utilisée pour toutes les élections fédérales, provinciales et municipales. Le personnel du Commissariat pourra sensibiliser les responsables aux dangers pour la vie privée que représenteraient par exemple la collecte de renseignements dans d'autres bases de données électroniques, ainsi que le mode d'accès à la liste, ses utilisateurs et ses mécanismes de sécurité, de même que l'exactitude et le degré de précision des données nécessaires.

Les vérificateurs constatent souvent que l'information sur les fonds de renseignements publiée dans *Info Source* est insuffisante, quand elle ne fait pas totalement défaut. Cette année, la tendance s'est maintenue. Il a été recommandé à toutes les institutions visées, sauf au Bureau de la sécurité des transports, de réviser, de compléter ou de modifier cette information publiée; elles ont toutes obtempéré.

Publier dans l'*Info Source* une information exacte et à jour est indispensable pour que chacun puisse exercer son droit d'accès à l'information et de correction des renseignements erronés. Quand l'information publiée est incomplète ou inexacte, l'administration gouvernementale est incapable de s'acquitter d'une des obligations fondamentales que la *Loi sur la protection des renseignements personnels* lui impose, à savoir de préciser quels renseignements elle recueille et comment elle les utilise et les communique.

Bureau du Directeur général des élections

En novembre 1994, le Commissariat terminait le suivi de la vérification qu'il avait menée en 1992 au Bureau du Directeur général des élections (Elections Canada). Cet organisme est chargé d'organiser les élections et les référendums fédéraux, ainsi que d'établir les listes électorales fédérales. Il a appliqué dix des onze recommandations du rapport de vérification, en faisant des changements administratifs et en modifiant la *Loi électorale du Canada*.

La seule recommandation en souffrance est celle qui porte sur l'évaluation, par la GRC, de la sécurité des systèmes de traitement électronique des données de l'organisme. Même si Elections Canada a renforcé ses mécanismes de contrôle à cet égard, ses systèmes n'ont pas encore été évalués par l'EIES afin de vérifier s'ils sont conformes aux pratiques de sécurité reconnues. L'organisme a assuré le Commissaire que l'évaluation se ferait sous peu. La sécurité de ces systèmes est critique, vu qu'Elections Canada veut établir une liste électorale permanente.

Cette année, le Commissariat a maintenu ses activités de suivi afin de s'assurer que les autorités responsables avaient appliqué les recommandations des vérifications antérieures. Les chefs de portefeuille se sont chargés de cette tâche pour neuf institutions; ils ont constaté que 37 des 39 recommandations (95 p. 100) avaient été intégralement appliquées, ce qui est un net progrès par rapport aux 77 p. 100 d'application de l'année précédente. Des deux recommandations qui n'avaient pas été intégralement appliquées, une l'avait été partiellement; l'autre est désormais sans objet.

Les institutions visées étaient Téléfilm Canada, le Bureau de la sécurité des transports, le Tribunal canadien du commerce extérieur, le Bureau du Directeur général des élections, la Société d'assurance-dépôt du Canada, Anciens combattants Canada, le Tribunal d'appel des anciens combattants, le Bureau des services juridiques des pensions et enfin le Bureau du Contrôleur général.

Ces institutions ont appliqué toutes les recommandations portant sur la sensibilisation de leur personnel. L'une d'entre elles s'est aussi dotée d'une politique pour assurer la confidentialité des renseignements personnels transmis par télécopieur. Une autre a réservé à son unité des ressources humaines une nouvelle imprimante, installée en lieu sûr pour empêcher ses autres employés d'avoir accès aux renseignements personnels de l'unité.

Environ la moitié des institutions devaient modifier leurs pratiques de conservation et de retrait pour se conformer à la *Loi sur la protection des renseignements personnels*. Toutes sauf une ont soumis des calendriers de conservation et de retrait aux Archives nationales pour approbation. Et un ministère effectuait des vérifications aléatoires pour qu'on n'envoie pas de documents de nature délicate au recyclage.

■ obtenir le consentement explicite des intéressés avant d'utiliser leurs noms et d'autres détails personnels à des fins d'envois postaux;

■ rédiger une politique de sécurité et revoir les pratiques susceptibles de saper la confidentialité des renseignements personnels qu'il détient;

■ faire évaluer la sécurité de son matériel et de ses systèmes informatiques par l'EIES de la GRC;

■ ajouter des clauses de protection de la vie privée dans les contrats qu'il signera avec des organismes de l'extérieur, afin de stipuler que tous les renseignements personnels recueillis ou générés dans ce contexte sont sa propriété exclusive;

■ donner des instructions précises sur le retrait sécuritaire du matériel informatique et des autres dispositifs de conservation de l'information avant de les jeter ou de les revendre;

■ empêcher le personnel des autres organisations avec lesquelles il partage les installations d'avoir accès aux renseignements personnels contenus dans ses bases de données ou dans son matériel de conservation de l'information;

■ sensibiliser son personnel à l'utilisation d'ordinateurs portatifs à l'extérieur de ses locaux, quand le disque dur contient des renseignements personnels, en équipant chacun de ces ordinateurs d'un dispositif de sécurité; et

■ établir un répertoire de tous ses fonds de renseignements personnels et de toutes ses listes de distribution postale, ainsi que vérifier l'exactitude de ses mentions dans *Info Source*.

Chaque année, il crée de 15 000 à 20 000 dossiers qui contiennent presque tous des renseignements personnels. Ses fonds de renseignements comprennent des données de base sur les artistes, les évaluateurs et les jurys, ainsi que des documents relatifs aux concours et aux demandes de subvention, y compris les observations des évaluateurs et des jurys sur les candidats. À cela s'ajoute toute la gamme des données sur le personnel.

La vérification devait avoir lieu l'an dernier, mais elle a été reportée à la demande du Conseil, qui a pourtant connu depuis une grosse réorganisation, doublée d'une compression d'effectif.

Les plus importantes recommandations portent sur la nécessité, pour le Conseil, de se donner des politiques et des procédures écrites de gestion des renseignements personnels, et de sensibiliser son effectif aux exigences de la *Loi sur la protection des renseignements personnels*.

En dépit des efforts que le Conseil a récemment déployés, ses employés ne comprennent toujours pas bien la notion de « renseignements personnels », et cette lacune se reflète dans la protection qu'ils accordent à ce genre d'information.

Le Commissaire a fait au Conseil des arts plusieurs recommandations sur la collecte, l'utilisation, la communication et la protection des renseignements personnels, dont :

- se donner une politique et des procédures écrites de gestion des renseignements personnels, et les distribuer à ses employés ainsi qu'aux évaluateurs de l'extérieur qui évaluent les demandes de subvention;

- revoir ses procédures et ses formulaires de collecte de renseignements, en ajoutant une déclaration sur les droits à la vie privée à tous ceux qui n'en contiennent pas déjà une;

Le Groupe a invité le chef de portefeuille à donner des conseils sur les questions de protection de la vie privée aux cadres supérieurs et au personnel responsable à l'occasion des réunions organisées dans le cadre de la refonte. Nous espérons faire état des progrès réalisés dans le rapport annuel de l'an prochain.

Administrations de pilotage du Pacifique et de l'Atlantique

Ces deux Administrations de pilotage fournissent des pilotes aux navires de haute mer voguant dans les eaux canadiennes et relevant de leur autorité. (Les Administrations de pilotage des Laurentides et des Grands Lacs ont fait l'objet d'une vérification en 1991.) La plupart des pilotes sont embauchés à contrat, de sorte que les Administrations recueillent et gèrent très peu de renseignements personnels. Leurs fichiers comprennent de l'information sur les certificats des pilotes, des renseignements médicaux et des rapports sur les accidents dans lesquels les pilotes auraient pu être impliqués. (Ils peuvent aussi contenir des renseignements sur l'inconduite des équipages de navires.)

Les vérificateurs ont recommandé aux Administrations d'ajouter des descriptions de leurs fichiers de données dans *Info Source* et de les modifier au besoin, d'améliorer leurs avis aux intéressés sur leur façon d'utiliser les renseignements personnels qui les concernent et de revoir leurs procédures de sous-traitance pour tenir compte des exigences de la *Loi sur la protection des renseignements personnels*. Les deux Administrations se sont engagées à prendre des mesures correctives.

Conseil des arts du Canada

Le Conseil des arts du Canada fournit aux artistes, aux professionnels des arts et aux organisations artistiques des fonds et des subventions pour encourager et promouvoir les arts au Canada. Il fait aussi office de Secrétariat de la Commission canadienne pour l'UNESCO.

- Les vérificateurs ont constaté des lacunes dans certains secteurs clés, mais en raison de la refonte en cours, ils ont limité leurs recommandations aux systèmes informatiques. Ainsi, il faudrait notamment :
- incorporer un code d'alerte dans le logiciel de gestion et de transmission des renseignements personnels inter-immeubles;
 - incorporer dans le logiciel d'extraction et d'impression des renseignements personnels des bases de données des commandes ajoutant automatiquement une déclaration sur la protection des renseignements personnels à chaque document imprimé, pour informer les utilisateurs des exigences de la Loi sur la protection des renseignements personnels;
 - évaluer les dangers et les risques de tous les systèmes informatiques et de tous les réseaux de communication;
 - faire inspecter les systèmes informatiques par l'EIES de la GRC, pour en évaluer la sécurité;
 - établir des critères écrits pour autoriser l'accès aux renseignements personnels contenus dans les systèmes informatiques;
 - créer un tracé de vérification dans les installations informatiques, afin de déterminer qui a eu accès à quels renseignements personnels et pour quelles raisons;
 - équiper tous les ordinateurs portatifs d'un codage permettant de protéger les renseignements personnels qu'ils contiennent en cas de perte ou de vol.

Le Commissaire a accepté la nouvelle définition et recommandé au Surintendant de la communiquer à tout le personnel des faillites, tout en modifiant les procédures de façon à protéger les autres renseignements personnels figurant dans les dossiers.

Immigration

Le personnel du Commissariat a terminé sa vérification au Groupe de l'immigration d'Emploi et Immigration Canada au cours de l'exercice financier 1993-1994. Malheureusement, il lui avait auparavant été impossible de faire état des résultats et de traiter de nombreuses questions qui restaient à trancher, en raison des perturbations qui ont entouré la réorganisation du Groupe et son intégration dans le nouveau ministère de la Citoyenneté et de l'immigration.

Les vérificateurs devaient étudier la façon du Groupe de traiter les renseignements personnels de son effectif et de sa clientèle, notamment dans plusieurs des 900 bureaux régionaux du Ministère. Le Groupe conserve dans 26 fichiers de données des renseignements personnels sur les 6,7 millions de personnes qui ont immigré au Canada depuis 1946.

Pour traiter et emmagasiner ces renseignements, le Groupe emploie deux gros systèmes informatiques, le SSOBL (Système de soutien aux opérations des bureaux locaux) et le SITCI (Système informatisé de traitement des cas d'immigration), ainsi que de nombreux sous-systèmes. Il est possible d'avoir accès aux données du SITCI de la plupart des bureaux canadiens des visas à l'étranger. Le Groupe est en train de refondre ses opérations, ce qui devrait influer nettement sur la gestion de ses dossiers et fichiers électroniques, et il consulte régulièrement le personnel du Commissariat quand aux implications de ses activités en matière de protection de la vie privée.

La difficulté portait sur une partie du contenu des documents publics conservés par le Surintendant des faillites.

La Loi sur la faillite et l'insolvabilité enjoint au Surintendant de conserver un registre public de toutes les procédures d'insolvabilité — faillites, propositions et mises sous séquestre. En outre, certains des fonctionnaires de son service font actuellement office de séquestres officiels. La Direction est donc en quelque sorte une cour d'archives, ce qui signifie que certains des documents relatifs aux affaires dont elle est saisie sont considérés comme publics, à l'instar de ceux qui sont déposés devant les tribunaux.

Certains des dossiers de faillites que les vérificateurs ont étudiés contenaient toute une gamme de renseignements personnels non seulement sur le failli, mais aussi sur les membres de sa famille et sur ses créanciers. Par exemple, certains dossiers contenaient des renseignements sur la consommation d'alcool de l'intéressé ou sur son obsession pour les paris, d'autres contenaient l'adresse personnelle, le numéro de téléphone et le numéro d'assurance sociale du créancier, quand c'était un particulier. Par ailleurs, le personnel du ministère n'a pas pu préciser aux vérificateurs quels renseignements personnels il leur fallait pour le registre public, ni à quels documents le public a accès.

Or, il est très important d'établir ce qui constitue un document public, étant donné que les dispositions de la Loi sur la protection des renseignements personnels sur l'utilisation et la communication, par les institutions, des renseignements personnels (articles 7 et 8) ne s'appliquent pas aux renseignements auxquels le public a accès.

Le Surintendant lui-même a examiné les dossiers en question pour définir précisément quels renseignements personnels doivent figurer dans le registre public et à quels documents le public peut accéder. Il s'est engagé à faire bénéficier tous les autres détails personnels des garanties de la Loi sur la protection des renseignements personnels.

déclaration de revenus de l'année précédente, ainsi qu'à ceux du Nord. Le NAS était bien visible sur l'enveloppe. Or, Revenu Canada n'avait pas besoin qu'il le soit, car le guide se serait rendu au destinataire même si le NAS n'avait pas figuré sur l'étiquette-adresse.

Les enquêteurs ont constaté que cette communication injustifiée était imputable à trois erreurs de traitement. Premièrement, les préposés auraient dû retirer le NAS des bandes informatiques qui avaient servi à préparer la liste de distribution avant d'envoyer celle-ci à l'imprimeur. Deuxièmement, Revenu Canada n'avait pas précisé quels renseignements devaient figurer sur l'étiquette. Enfin, le personnel aurait dû vérifier des échantillons d'étiquettes avant de donner le feu vert à l'expédition.

Revenu Canada reconnaît qu'il lui incombe de protéger la confidentialité du NAS. Le sous-ministre s'est personnellement intéressé à l'affaire, et le Ministère a rapidement pris des mesures pour éviter un nouvel incident.

Vérifications et suivi

Cette année, le personnel a mené à bien deux importantes vérifications, l'une au ministère de la Consommation et des Corporations et l'autre au volet Immigration d'Emploi et Immigration (les deux ont depuis été incorporés dans de nouveaux ministères), de même que des vérifications de moindre envergure au Conseil des arts du Canada ainsi qu'à l'Administration de pilotage de l'Atlantique et à celle du Pacifique—ce qui conclut les travaux de vérification dans les quatre Administrations de pilotage.

Consommation et Corporations

Le Commissariat a terminé son étude du dernier point en suspens de sa vérification de 1993-1994 de Consommation et Corporations Canada (devenu depuis un des éléments d'Industrie Canada).

Le SCC était mêlé à six des dix enquêtes sur des incidents entreprises par le Commissariat au cours de l'année à l'étude. Dans chaque cas, l'enquête a résulté d'une erreur de traitement de renseignements personnels.

Coordonnées d'une dame communiquées à un détenu

Dans un des six cas, le SCC a écrit à une dame qui voulait obtenir des renseignements sur un membre de sa famille. Un employé a mis par erreur la lettre destinée à la dame dans une enveloppe adressée à un détenu, qui purgeait une peine de prison pour des crimes violents perpétrés contre des femmes, dans un pénitencier situé près de la résidence de l'intéressée.

Même si ce détenu ne sera pas libéré avant plusieurs années, le personnel du Commissariat craignait que cette erreur ne mette vraiment la dame en danger.

Le SCC a volontiers reconnu son erreur. À la demande du Commissariat, un fonctionnaire du SCC s'est rendu voir l'intéressée pour lui expliquer ce qui s'était produit et pour l'informer de la situation. Il semble que la dame n'était pas très inquiète; elle n'a pas voulu que le SCC prenne d'autres mesures. Par ailleurs, le SCC s'est engagé à modifier ses procédures de distribution postale pour éviter que cela ne se reproduise.

Des NAS sur des enveloppes...

Revenu Canada a suscité plusieurs plaintes en envoyant à plus de 700 000 contribuables un guide d'impôt spécial, car le numéro d'assurance sociale des destinataires figurait sur l'étiquette-adresse.

Le Commissariat a été saisi du problème par un journaliste, puis par plusieurs des personnes qui avaient reçu cet envoi. Les étiquettes en question avaient été apposées sur l'enveloppe de guides livrés par la poste aux contribuables qui avaient déclaré un revenu locatif dans leur

actions, ou encore celles de leur personnel, en prétendant le faire pour protéger leur vie privée; ni l'un, ni l'autre des deux organismes ne le fait, d'ailleurs.

Il faut vraiment concilier des intérêts divergents pour appliquer les dispositions sur la communication des renseignements. L'intérêt public, c'est plus que de la curiosité. L'institution doit démontrer comment cet intérêt doit prévaloir sur les droits individuels à la vie privée. Il faut y réfléchir sérieusement, même lorsque la communication est justifiée.

Enquêtes sur les incidents

Les chefs de portefeuille ont aussi fait enquête sur dix incidents susceptibles de s'être conclus par la perte, le vol ou la communication non autorisée de renseignements personnels.

Les lecteurs fidèles du Rapport annuel se rappellent peut-être que la plupart des incidents des années antérieures semblaient mettre en cause une poignée seulement d'institutions : Service correctionnel Canada, la Commission nationale des libérations conditionnelles, Anciens combattants Canada et Revenu Canada. Cette année ne fait pas exception.

Cela ne veut pas dire que les pratiques de gestion de l'information des autres ministères et organismes sont meilleures au point qu'ils ne perdent jamais de renseignements personnels, qu'ils ne les communiquent jamais indûment ou qu'ils ne s'en font pas voler. En fait, les institutions susmentionnées comptent parmi les rares qui prennent leurs responsabilités en informant le Commissaire que des renseignements personnels n'ont peut-être pas été protégés comme il se doit. Aviser le Commissaire a son bon côté, car c'est l'occasion pour le personnel des programmes d'obtenir l'aide du Commissariat afin de corriger une lacune (et d'empêcher qu'un incident ne se reproduise).

Aviser le Commissaire

Communications dans l'intérêt public

Le nombre d'avis de communication a légèrement augmenté, passant à 56 comparativement à 48 l'an dernier. Certains ministères et organismes, dont Service correctionnel Canada (SCC), qui a envoyé à lui seul 22 des 56 avis reçus cette année, commencent à se prévaloir systématiquement des dispositions pertinentes.

La grande majorité des avis de communication du SCC résultaient de demandes des médias fondées sur la *Loi sur l'accès à l'information* afin d'obtenir des rapports internes sur des évasions de détenus ou sur des incidents violents dans les pénitenciers. Ces rapports contiennent habituellement des renseignements personnels sur les détenus, les victimes et le personnel, et fréquemment aussi une analyse des facteurs qui déterminent dans quels pénitenciers les détenus sont incarcérés, ainsi que les conditions de leur libération.

Le public s'intéresse de plus en plus à la détermination de la peine et aux libérations conditionnelles, particulièrement dans le cas des criminels dangereux, de sorte que SCC subit des pressions pour exposer tous les facteurs qui influent sur ses décisions et sur celles de la Commission nationale des libérations conditionnelles (CNLC), dans ce contexte. En outre, chaque fois qu'un incident arrive—par exemple lorsqu'un détenu commet un meurtre lorsqu'il est en semi-liberté—SCC estime que le public a le droit d'obtenir toute l'information sur ce qui aurait pu contribuer à l'incident. Souvent, cela signifie qu'on communique beaucoup de renseignements personnels délicats; parfois, SCC va trop loin par souci d'ouverture et d'imputabilité.

Néanmoins, nous savons depuis longtemps qu'on ne peut invoquer dans son propre intérêt les exceptions à la règle de la protection des renseignements personnels. SCC et la CNLC ne doivent pas refuser de communiquer de l'information qui critique leurs décisions ou leurs

nécessiteux des prestations pour la période de carence obligatoire de trois semaines de l'assurance-chômage (à laquelle il faut parfois ajouter deux ou trois semaines pour le traitement de la demande). Les demandeurs doivent signer un formulaire pour confirmer qu'ils s'engagent à rembourser les prestations d'assurance-chômage versées en sus de leurs prestations d'aide sociale.

Permettre aux déposés des programmes d'aide sociale d'avoir directement accès à cette information libère le personnel de DRH, qui n'a plus à répondre à de nombreuses demandes de ces déposés, tout en faisant gagner du temps à ces derniers et en évitant aux demandeurs de devoir aller d'un bureau à l'autre.

programmes; elle a suggéré des pertes de plus de 20 millions de dollars par année.

DRH a conclu qu'il était à la fois faisable et rentable de coupler régulièrement les deux bases de données, puis a soumis l'évaluation du couplage au Commissaire. L'évaluation et les discussions entre le personnel du Commissariat et celui de DRH ont révélé que les avantages du couplage de données l'emportent manifestement sur le préjudice qui résulterait d'une éventuelle violation de la vie privée des intéressés. En effet, les prestataires signent un formulaire pour attester qu'ils consentent à ce que l'information qu'ils fournissent dans les formules de demande soit vérifiée.

Indemnités d'accidents du travail et prestations d'assurance-chômage : DRH a réalisé une autre étude, portant celle-là sur les personnes qui touchaient en même temps des prestations de la Commission des accidents du travail de l'Ontario et de l'assurance-chômage.

Cette étude a elle aussi supposé des paiements en trop pouvant totaliser des pertes de plus de 20 millions de dollars par année. Après avoir été informé du couplage et l'avoir évalué, le Commissaire l'a approuvé. Dans ce cas-là aussi, les avantages l'emportent clairement sur le risque de préjudice résultant d'une violation de la vie privée des intéressés.

Dans le troisième cas, il ne s'agissait pas à proprement parler d'un couplage de données, mais plutôt de modifications d'un protocole d'échange d'information. Bien que rien ne l'oblige à le faire, DRH a décidé de consulter le Commissariat pour éviter toute difficulté.

Services sociaux de l'Ontario et assurance-chômage : Les

préposés aux services sociaux municipaux peuvent avoir désormais directement accès, grâce à des terminaux réservés, à des données personnelles limitées contenues dans la base de données de l'assurance-chômage de DRH, ce qui leur permet de vérifier si ceux qui réclament des prestations d'aide sociale ont demandé à bénéficier de l'assurance-chômage. Les programmes provinciaux d'aide sociale fournissent aux

Avant d'aller de l'avant avec un couplage de données, l'institution doit démontrer que :

- les renseignements ne peuvent pas être obtenus par d'autres méthodes;
- leur collecte est directement liée à un de ses programmes en cours;
- la collecte directe des renseignements serait contre-indiquée;
- les renseignements seront exacts, à jour et complets, et
- les avantages du couplage de données l'emportent clairement sur le préjudice que causerait une violation de la vie privée des intéressés.

Trois programmes à Développement des ressources humaines

Trois cas récents à Développement des ressources humaines Canada (DRH) montrent bien comment l'administration fédérale, les gouvernements provinciaux et les autorités municipales partagent des renseignements personnels pour lutter contre les fraudeurs de l'assurance-chômage ainsi que des programmes provinciaux et municipaux d'aide sociale.

Assurance-chômage et Régime de pensions du Canada : DRH a réalisé une étude de faisabilité afin d'estimer les pertes attribuables aux paiements versés à des personnes qui avaient réclamé des prestations à la fois d'assurance-chômage et d'invalidité du Régime de pensions du Canada. (Quiconque touche des prestations d'invalidité du RPC est incapable de travailler et n'a donc pas droit à l'assurance-chômage....) L'étude consistait à coupler des listes des prestataires des deux

L'analyse des résultats a révélé que 47 des répondants ne font aucun partage interne ni externe de renseignements, 2 des échanges internes, 17 des échanges externes mais pas internes, 27 des échanges internes et externes, tandis que 18 font du couplage de données.

Le second volet de l'étude doit vérifier la fiabilité des données et se concentrer sur un certain nombre d'accords et d'ententes. Par ailleurs, le Commissariat va élaborer des lignes directrices afin d'être plus en mesure, l'an prochain, de donner des conseils sur le partage de renseignements aux institutions fédérales.

Couplage de données

Le couplage des données est une technique que les administrations gouvernementales emploient fréquemment pour partager des renseignements. Fondamentalement, il consiste à comparer des renseignements personnels provenant de différentes sources afin de prendre des décisions sur les prestations ou les services dont les intéressés bénéficient. Au départ, il se résument à des échanges de bandes informatiques, mais il tend de plus en plus à permettre à d'autres utilisateurs — autres éléments d'une même organisation ou autres gouvernements — d'avoir accès sans intermédiaire et en direct à des bases de données.

L'administration fédérale a adopté en 1989 une politique qui enjoint aux organismes gouvernementaux de faire des évaluations détaillées des couplages de données qu'ils envisagent et d'en informer préalablement le Commissaire. Néanmoins, les couplages ne sont toujours pas déclarés, et il n'existe aucun mécanisme grâce auquel le Commissaire pourrait évaluer l'ampleur des activités de couplage de données de l'administration fédérale.

ensemble des ministères et organismes. Cette année, l'exercice a porté sur le partage des renseignements personnels avec d'autres programmes ou d'autres organisations.

Il est fondamental de connaître la nature des renseignements personnels que le gouvernement partage, sa façon de les partager et l'identité des organisations intéressées, aussi bien pour que le droit de chacun à la vie privée soit protégé que pour assurer l'efficacité du contrôle exercé par le Commissaire. Or, bien que la *Loi sur la protection des renseignements personnels* interdise au gouvernement d'utiliser ces renseignements à d'autres fins que celles pour lesquelles ils ont été collectés (article 7), elle autorise leur communication dans bien des circonstances (article 8).

Par exemple, les institutions fédérales peuvent conclure des accords ou des ententes en vue de partager des renseignements avec un autre gouvernement (ou l'une de ses organisations), pour l'application de lois ou la tenue d'enquêtes licites.

Le Conseil du Trésor a publié des lignes directrices sur les accords de partage de renseignements, mais il n'a donné aucune définition de ce qui constitue une « entente ». En outre, les ministères et organismes ne sont pas tenus d'informer le Commissaire lorsqu'ils concluent un accord, alors qu'ils doivent le faire dans les cas de couplage de données.

Au début de 1995, le Commissariat a fait un sondage parmi les 10 institutions assujetties à la *Loi sur la protection des renseignements personnels* afin de déterminer l'étendue de leurs échanges de leurs couplages de renseignements personnels. Le questionnaire du sondage, en quatre parties, avait été conçu pour que les répondants déclarent tous leurs accords ou tous leurs arrangements de couplage et l'échange de données, tant internes qu'externes, et 93 des institutions sollicitées ont répondu.

■ Le Secrétariat du Conseil du Trésor va écrire à tous les sous-ministres adjoints pour leur demander de veiller à ce que leurs organisations appliquent des procédures visant à prévenir toute communication non autorisée de renseignements protégés ou désignés, notamment dans le contexte de la disposition du matériel excédentaire.

■ Enfin, le Conseil du trésor et le Centre de disposition des biens de la Couronne ont convenu de sensibiliser les responsables de la gestion du matériel de l'administration fédérale à la question, dans les publications qui leur sont distribuées.

L'entente ne mettra pas nécessairement fin à la

communication de renseignements par simple manque de précautions.

Néanmoins, elle devrait au moins faire en sorte que les ministères et organismes gouvernementaux se donnent les mécanismes de protection voulus et sensibilisent leurs employés aux dangers de bâcler la disposition de leur matériel excédentaire.

Cela dit, l'administration fédérale va maintenant devoir en faire autant pour veiller à ce qu'on ne puisse pas récupérer les données emmagasinées sur les disques durs, les bandes et les disquettes endommagées au point d'être inutilisables. Il ne suffit pas de les envoyer au dépôt, car quiconque connaît l'informatique peut extraire une partie de l'information mémorisée. Autrement dit, même ce matériel-là doit être effacé ou détruit pour qu'on ne puisse pas récupérer l'information.

Partage de renseignements personnels— accords et ententes

Le Commissariat a commencé cette année à maximiser l'exploitation de ses ressources limitées de vérification en adoptant une approche systémique, c'est-à-dire en se concentrant sur un aspect seulement de la façon de traiter les renseignements personnels dans

Enfin, les ordinateurs désuets sont envoyés au programme des Ordinateurs pour l'école d'Industrie Canada. L'an dernier, les responsables du programme ont déclaré qu'environ 95 p. 100 de tous les ordinateurs qu'ils avaient reçus contenaient encore des données et des programmes, en dépit des directives gouvernementales ordonnant que l'on efface les disques durs et les disquettes. Cette année, les nouvelles sont plus encourageantes, puisque de 35 à 45 p. 100 de tous les ordinateurs fédéraux donnés au programme ne contenaient pas de données. C'est mieux, mais il reste encore du chemin à faire : les 55 à 65 p. 100 restants contiennent encore beaucoup de données gouvernementales.

L'entente conclue prévoit que :

■ Le Centre va modifier le formulaire sur laquelle les institutions fédérales inscrivent les articles à vendre, en leur imposant l'obligation d'attester qu'ils ne contiennent plus de renseignements délicats ou protégés. La version modifiée du formulaire doit être publiée en juillet 1995.

■ Le Centre va informer les ministères et organismes clients de cette modification en leur envoyant un avis ou un bulletin, en plus d'afficher la modification dans tous ses bureaux au Canada et de modifier son manuel des clients.

■ Une fois opérationnel, le babillard électronique à l'intention des gestionnaires gouvernementaux du matériel comprendra un message permanent rappelant à quiconque vend ou échange des biens excédentaires de s'assurer qu'ils ne contiennent plus de renseignements de nature délicate.

■ La GRC a envoyé à tous les ministères et organismes des bulletins décrivant un logiciel approuvé par la GRC et capable d'effacer toutes les données des disques durs. Pour le reste, elle ne peut que continuer à rappeler qu'il faudrait effacer les disques durs des vieux ordinateurs avant de s'en débarrasser.

Il n'a pas été facile de savoir exactement à qui incombe la responsabilité de retirer tous les renseignements des classeurs, des ordinateurs et des disquettes avant de les revendre, car les intéressés tendent dans bien des cas à la refiler aux autres. Pour que des mesures concrètes soient prises, nous avons dû obtenir la collaboration du Conseil du Trésor, du Centre de distribution des biens de la Couronne, de la GRC et des ministères intéressés.

Le Commissariat n'a pas cessé d'insister auprès des principaux intervenants avant d'avoir obtenu une entente.

Qui fait quoi?

Les responsabilités se répartissent de la façon suivante : le Centre de disposition des biens de la Couronne est en théorie le dernier point de transit du matériel revendu, mais il n'a pas suffisamment de personnel pour s'assurer que on a retiré ou effacé tous les renseignements délicats contenus dans le matériel excédentaire, de sorte que cette responsabilité incombe au ministère ou à l'organisme qui en était propriétaire. En fait, il arrive souvent que les meubles ou les classeurs de surplus ne passent même pas par le Centre, qui fait alors simplement office d'aiguilleur pour dire aux acheteurs éventuels à quels ministères s'adresser pour obtenir le matériel disponible.

C'est la Section des techniques de sécurité de la GRC qui ouvre les coffres-forts excédentaires et rétablit la combinaison originale de l'usine avant de les envoyer au Centre; celui-ci part du principe qu'ils sont vides, sans vérification.

Par ailleurs, six ministères participent à un projet pilote qui leur permettra de disposer de leur propre équipement excédentaire en le donnant en échange de matériel neuf et en faisant des transferts interministériels, le tout sans prévenir le Centre.

projets d'échange d'information avec les autres ministères, organismes, gouvernements ou le secteur privé. Une fois qu'ils ont bien saisi ces implications, ils ne sont que trop heureux de demander conseil pour éviter d'avoir des problèmes.

Deux exemples illustrent bien les avantages à examiner les questions de l'heure à l'échelle de tout le gouvernement; il s'agit de l'allocation des biens excédentaires et du partage des renseignements personnels avec les autres organismes et gouvernements.

Aliénation des biens excédentaires de l'État

L'histoire se répète, car cette pratique n'a toujours pas attiré l'attention qu'elle mérite : dans le Rapport annuel de 1992-1993, nous avons raconté l'histoire d'un ancien employé du Commissariat qui avait acheté un classeur d'occasion contenant — à sa grande surprise — des centaines de fiches d'analyse de laboratoire personnelles. Eh bien, la poudre a frappé au même endroit cette année. Le Commissariat a trouvé plusieurs documents de la GRC, dont des plans d'urgence secrets et des évaluations de rendement de hauts grades de la Gendarmerie, dans un coffre-fort dont il venait de faire l'acquisition au Centre de distribution des biens de la Couronne.

En octobre, un homme a trouvé des disquettes usagées renfermant des renseignements confidentiels sur des personnes inscrites à la TPS dans un classeur qu'il avait acheté à une vente de matériel excédentaire de l'État. Ces incidents mettant en cause l'administration fédérale ne sont que des exemples des nombreux cas signalés dans les médias de documents laissés sans protection dans des classeurs, des ordinateurs et des disquettes excédentaires.

Il a été difficile pour le personnel du Conseil du Trésor et du Commissariat de retracer des dossiers et de suivre les décisions reliées à des renseignements personnels ayant depuis été transférés.

Vers un système de portefeuilles

Le Commissariat a dû réduire ses vérifications de routine de l'observation de la Loi par le gouvernement, en raison de la charge de travail nettement exagérée qu'elles représentent pour les quatre personnes affectées à cette tâche. Nous avons maintenant des chefs de portefeuilles qui s'efforcent de développer une bonne compréhension des activités des organismes et des programmes afin d'agir comme contact initial pour le personnel gouvernemental. Cette approche, plus active, vise à prévenir les problèmes qui pourraient survenir au sein d'un organisme en matière de vie privée, et à offrir des solutions plus globales que ponctuelles.

Depuis qu'il a instauré le système des portefeuilles, le Commissaire a écrit à tous les administrateurs généraux pour leur exposer la nouvelle approche du Commissariat et pour leur offrir ses services. L'accueil a été enthousiaste. Les chefs de portefeuille ont rencontré plus de coordonnateurs de la protection de la vie privée représentant plus de 80 ministères et organismes fédéraux pour leur donner des exposés, en plus d'animer des séances d'information pour plus de 400 personnes, cadres supérieurs, spécialistes, employés des services correctionnels et représentants d'une entreprise privée travaillant à un important projet de refonte des systèmes informatiques.

Le personnel du Commissariat a eu beaucoup à faire pour répondre à une kyrielle d'appels pour obtenir des explications sur la Loi et sur sa politique d'application dans diverses situations. Il arrive souvent que les gestionnaires ne s'intéressent pas beaucoup à la protection de la vie privée avant de constater tout son impact sur les relations du travail, sur la conception des systèmes informatiques et sur les fonds de renseignements, sur les renseignements personnels concernant leurs clients et leurs employés, ainsi que sur les

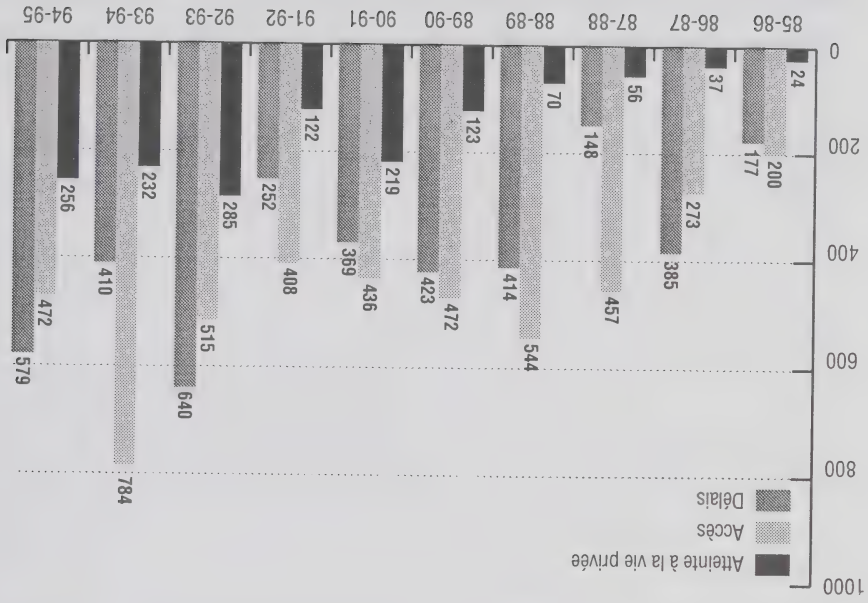
Vérification de l'observation

Les répercussions de la restructuration gouvernementale à l'échelle fédérale ont été fortement ressenties cette année. À la réorganisation de juin 1993, dont nous faisons état l'année dernière, a suivi la revue des programmes, soit une réévaluation totale de chaque programme et activité à l'échelle fédérale (dont plus de 400 agences, conseils et commissions). Cet exercice a été suivi en février 1995 de l'annonce du budget et par la fermeture de 73 agences, du dégraisage de 47 autres et de coupures en personnel de l'ordre de 45 000 employés, dont 20 000 d'ici l'été 1996.

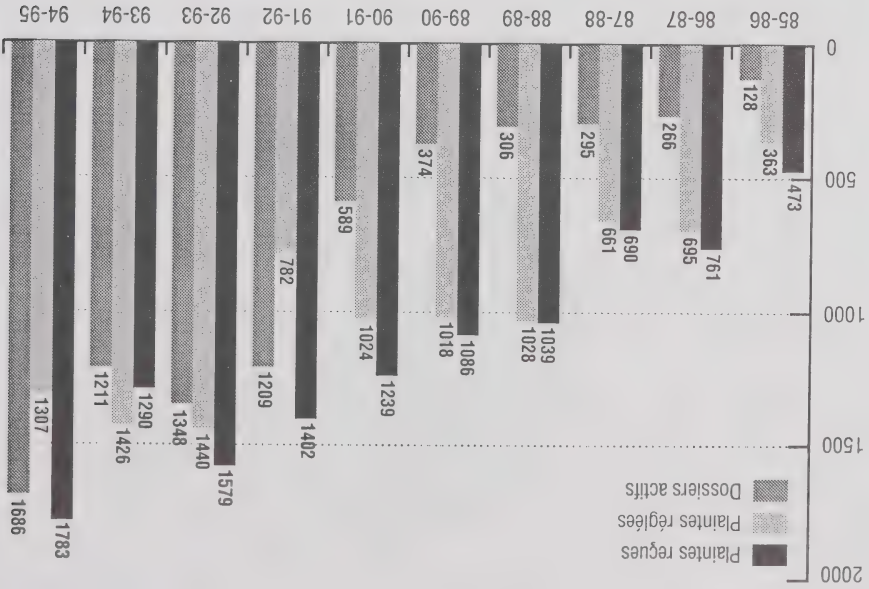
Au niveau des ministères, le personnel affecté au traitement des demandes de renseignements personnels n'a pas été épargné. Mais la charge de travail n'a pas diminué; elle a simplement été répartie entre ceux qui restaient. On pouvait facilement en prévoir les répercussions. Incapable de répondre dans les 30 jours prévus, le personnel a accumulé du retard dans le traitement des demandes et en conséquence, les plaintes de délais déposées auprès du Commissariat s'accroissent régulièrement. Ces délais comptent pour quelque chose dans le nombre grandissant de plaintes dont le Commissariat est saisi.

L'étendue des changements a amené les ministères à refaire ou intégrer à la sauvette divers systèmes informatisés, à déménager des dossiers de clients et d'employés et à décider comment emmagasiner ou éliminer des renseignements personnels qui n'ont plus d'appartenance en tant que telle.

Le suivi des vérifications antérieures s'est trouvé, à la suite de la réorganisation, rendu encore plus complexe puisque des recommandations qui s'appliquaient aux vieilles unités de travail doivent maintenant être expliquées aux gestionnaires qui ont hérité de ces programmes (ou qui les ont perdus dans le remue-ménage). Ainsi, en 1992 une vérification avait été faite au bureau du Contrôleur général, mais celui-ci a subi une refonte avec le Secrétariat du Conseil du Trésor.

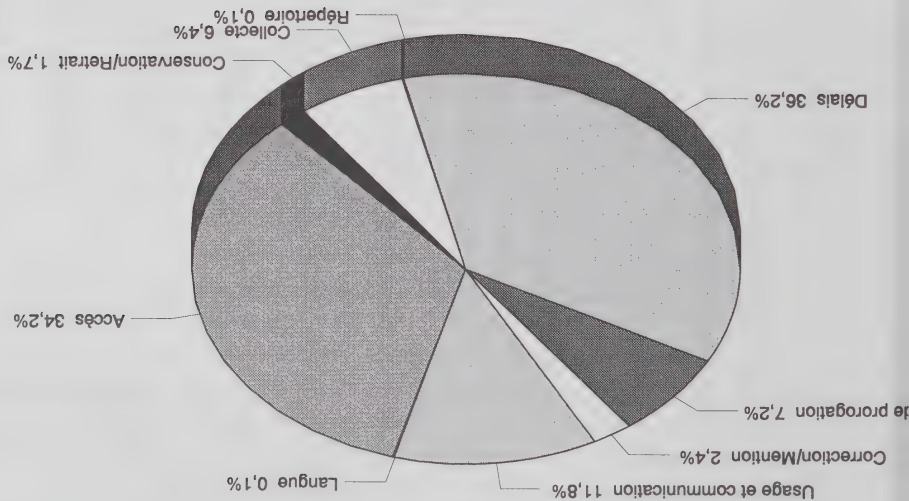


Plaintes réglées et motifs 1985-1995



Plaintes réglées 1985-1995

Plaintes réglées par motifs



Origine des plaintes réglées

Origine	Nombre de plaintes
Terre-Neuve	8
Ile-du-Prince-Édouard	3
Nouvelle-Écosse	36
Nouveau-Brunswick	25
Québec	112
Région de la Capitale nationale - Québec	12
Région de la Capitale nationale - Ontario	240
Ontario	438
Manitoba	35
Saskatchewan	63
Alberta	76
Colombie-Britannique	233
Territoires du Nord-Ouest	3
Yukon	1
Hors Canada	22
TOTAL	1307

Plaintes réglées par institutions et résultats

Institution	Nombre	Bien-fondée	Bien-fondée; résolue	Non fondée	Abandonnée	Résolue
Finances, Ministère des	1	0	0	1	0	0
Gendarmerie royale du Canada	100	5	11	83	1	0
Industrie, Science et Technologie	5	1	0	4	0	0
Justice, Ministère de la	12	5	4	3	0	0
Monnaie royale canadienne	3	0	0	3	0	0
Pêches et Océans	5	5	0	0	0	0
Revenu Canada	189	116	12	60	1	0
Santé Canada	31	7	7	16	1	0
Secrétariat d'État du Canada	4	1	1	2	0	0
Service canadien du renseignement de sécurité	51	0	0	51	0	0
Service correctionnel Canada	195	72	12	101	10	0
Société canadienne d'hypothèques et de logement	2	0	0	2	0	0
Société canadienne des Ports	2	0	1	1	0	0
Société canadienne des Postes	99	9	14	67	9	0
Société du crédit agricole Canada	1	0	0	1	0	0
Solliciteur général Canada	4	0	0	4	0	0
Statistiques Canada	27	1	0	0	0	26
Transports Canada	10	0	3	7	0	0
Travaux publics et Services gouvernementaux Canada	1	0	0	0	1	0
TOTAL	1307	470	125	645	41	26

Plaintes réglées par institutions et résultats

Institution	Nombre	Bien- fondée	Bien- fondée; résolue	Non fondée	Abandon- née	Résolue
ffaires des anciens combattants Canada	1	0	0	1	0	0
ffaires étrangères et Commerce International Canada	1	0	0	1	0	0
ffaires indiennes et du Nord Canada	44	21	1	22	0	0
gence Spatiale Canadienne	3	1	0	2	0	0
griculture Canada et Agro-alimentaire	39	20	5	12	2	0
rchives Nationales du Canada	14	0	1	12	1	0
anque du Canada	1	0	0	1	0	0
ureau de la sécurité des transports du Canada	5	0	0	5	0	0
ureau du Conseil Privé	7	3	1	3	0	0
oyenneté et immigration Canada	45	31	1	7	6	0
ommission canadienne des droits de la personne	4	0	2	2	0	0
ommission de l'immigration et du statut du réfugié	39	6	13	20	0	0
ommission de la Fonction publique du Canada	6	2	3	1	0	0
ommission des plaintes du public contre la GRC	5	0	0	5	0	0
ommission nationale des libérations conditionnelles	26	3	6	16	1	0
omité de surveillance des activités de renseignement de sécurité	1	0	0	1	0	0
ommunications, Ministère des	1	0	1	0	0	0
Conseil canadien des relations de travail	7	2	2	3	0	0
Conseil du Trésor du Canada, Secrétariat	2	2	0	0	0	0
Défense nationale	162	88	13	60	1	0
Développement des ressources humaines Canada	51	20	4	21	6	0
Élections Canada	2	0	0	2	0	0
Emploi et Immigration Canada	89	43	7	38	1	0
Énergie, Mines et Ressources Canada	1	0	0	1	0	0
Enquêteur correctionnel Canada, L'	1	0	0	1	0	0
Environnement Canada	8	5	0	3	0	0

Les dix ministères les plus visés selon les plaintes reçues

Motifs				
Ministère	Total	Accès	Délais	Vie privée
Service correctionnel Canada	331	148	136	47
Défense nationale	274	62	164	48
Revenu Canada	237	48	147	42
Gendarmerie royale du Canada	154	76	44	33
Développement des ressources humaines Canada	150	42	52	56
Citoyenneté et immigration Canada	129	26	90	13
Service canadien du renseignement de sécurité	101	95	4	2
Société canadienne des Postes	97	52	20	25
Commission de l'immigration et du statut de réfugié	34	15	16	3
Commission nationale des libérations conditionnelles	26	16	9	1
AUTRE	250	120	47	80
TOTAL		1783	704	350

Plaintes réglées par motifs et résultats

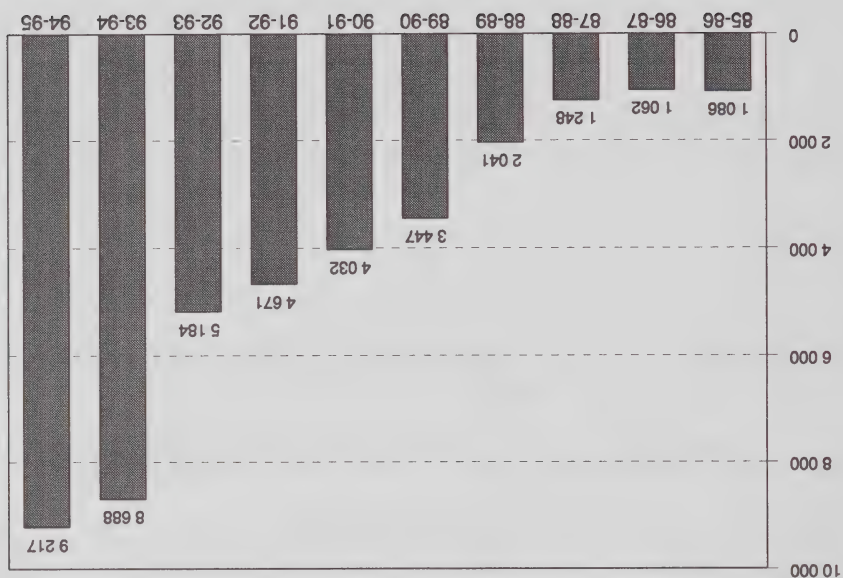
Accès		Motifs		Bien-fondée	Bien-fondée; résolue	Non fondée	Résolue	Abandon-née	TOTAL
				17	105	329	0	21	472
Accès				13	100	306	0	20	439
Correction/Annotation				4	5	22	0	0	31
Frais contre-indiqués				0	0	0	0	0	0
Répertoire				0	0	1	0	0	1
Langue				0	0	0	0	1	1
Atteinte à la vie privée				58	14	141	26	17	256
Collecte				4	4	40	26	8	82
Conservation/Retrait				13	0	9	0	0	22
Usage et Communication				41	10	92	0	9	152
Délais				394	6	176	0	3	579
Correction/Délai				21	0	1	0	0	22
Délais				354	6	102	0	3	465
Avis de prorogation				20	0	72	0	0	92
TOTAL				469	125	646	26	41	1307

Commissariat conseille aux employés d'essayer de résoudre le problème avec les préposés aux ressources humaines de leur entreprise ou avec leur syndicat.

Par ailleurs, plusieurs personnes se sont plaintes au Commissariat d'être incapables d'avoir accès à leurs dossiers médicaux ou psychologiques; elles ont été priées de s'adresser plutôt au Collège royal des Médecins et Chirurgiens.

Le tableau suivant illustre l'augmentation du nombre de demandes de renseignements traitées.

Demandes de renseignements 1985-1995



leur NAS dans ses dossiers et continuer à l'utiliser pour les mêmes fins.

Le Commissaire a parlé de ces renonciations totales lorsqu'il a récemment comparu devant le Comité sénatorial des banques, qui est chargé de surveiller l'industrie financière. La confidentialité des documents concernant la clientèle est l'une des questions auxquelles le Comité s'attache, en raison des modifications apportées à la législation régissant les banques ainsi que les compagnies de fiducie et d'assurance.

Entrée des données personnelles sur l'autoroute de l'information

Le battage publicitaire qui entoure l'autoroute de l'information—et la confusion qui en résulte—ont incité bien des gens à demander conseil au Commissariat pour mieux se protéger, en raison de l'absence de protection légale dans le secteur privé. Or, le Commissariat ne peut leur donner que des conseils généraux lorsqu'il s'agit de transmettre des données personnelles sur les réseaux interactifs :

■ partez du principe que le système n'est pas protégé, à moins que l'exploitant ne puisse prouver le contraire, et ne transmettez pas de renseignements personnels que vous ne voudriez pas que tout le monde connaisse;

■ ne révélez pas vos numéros de cartes bancaires ni d'autres renseignements financiers, à moins que le système ne les code;

■ demandez aux exploitants de groupes d'utilisateurs comment ils emmagasinent et utilisent les renseignements personnels que vous leur fournissez pour vous identifier en tant qu'utilisateur légitime; sont-ils protégés?

Dans un autre ordre d'idées, le Commissariat a reçu près de 1 000 demandes de renseignements au sujet d'entreprises privées qui affichent en public les paiements d'heures supplémentaires, le NAS, l'adresse et d'autres renseignements personnels concernant leurs employés. Or, c'est peut-être manquer de délicatesse, mais ce n'est pas illégal (sauf peut-être au Québec, qui s'est donné une loi de protection des renseignements personnels dans le secteur privé). Dans ces cas-là, le

Demandes de renseignements

Le Commissariat a répondu pendant l'année à 9 217 demandes de renseignements, soit 529 de plus que l'année précédente.

Même si deux agents répondent à temps plein aux demandes, la charge de travail est telle que virtuellement tout le personnel doit pousser à la roue, en donnant des explications sur la *Loi sur la protection des renseignements personnels* et la procédure de plainte, en plus de fournir des renseignements élémentaires sur les questions de vie privée qui ne relèvent pas du Commissariat, ainsi qu'en aiguillant les correspondants vers d'autres organismes gouvernementaux ou vers le secteur privé, le cas échéant. Les agents des demandes de renseignements sont aussi chargés de déterminer si le problème relève de la compétence du Commissaire et s'il peut faire l'objet d'une enquête, auquel cas ils constituent le premier palier de réception des plaintes.

Demande de carte Visa Or

Le Commissariat a reçu plus de 100 appels à cause de la nouvelle formule de demande de carte Visa Or de la Banque Royale, dans laquelle on demande aux clients d'autoriser la Banque à utiliser leur numéro d'assurance sociale pour toute une gamme de services. Les clients des institutions financières sont tenus par la *Loi de l'impôt sur le revenu* de fournir leur NAS à ces institutions afin qu'il puisse figurer dans les relevés d'intérêts. Par contre, elle interdit à ces mêmes institutions d'utiliser le NAS à d'autres fins sans le consentement des clients. Malheureusement, la demande de consentement de la Banque Royale est rédigée en termes tellement larges qu'elle équivaut virtuellement à une renonciation totale de la protection prévue par la *Loi de l'impôt sur le revenu*. Ainsi, les clients s'engagent à ce que :

■ la Banque puisse considérer comme un renseignement leur NAS, s'ils le lui ont déjà donné, et l'autorisent à l'utiliser pour qu'il soit plus facile de les identifier auprès des bureaux de crédit et d'autres parties.

■ en outre, même si les clients cessent d'avoir recours aux services de la Banque (ou si l'accord contracté dans la demande de carte vient à échéance), celle-ci peut conserver

Atin que le nom du plaignant ne déclenche plus l'alerte, Agriculture Canada a retiré les renseignements qui le concernent du SRRJ et va cesser d'inscrire dans le système les renseignements n'ayant rien à voir avec l'application de la loi, en plus d'en retirer ceux qui y figurent déjà. Ces mesures devraient éviter que d'autres personnes se retrouvent avec le même problème que le plaignant.

Nouveau système informatisé de surveillance des Douanes

Une personne de la Nouvelle-Écosse a fini par découvrir pourquoi on le retenait pour le soumettre à un interrogatoire en règle chaque fois qu'il franchissait la frontière canado-américaine : son nom figurait dans le nouveau Système automatisé de surveillance des Douanes.

Le Système de surveillance contient les noms des personnes qui ont, ou qui sont soupçonnées d'avoir, enfreint l'une des lois que les Douanes appliquent à la frontière du Canada, dont en matière d'immigration, d'agriculture et de contrôle des armes à feu. Notre homme s'est plaint au Commissaire en déclarant que Revenu Canada n'aurait pas dû recueillir ces renseignements.

Le Système de surveillance des Douanes partage certains renseignements avec le Système de récupération des renseignements judiciaires (SRRJ), une base de données de la GRC contenant des renseignements sur toute une gamme d'événements, de sujets, de véhicules et de biens. La GRC met son système à la disposition d'autres ministères et organismes fédéraux. Il semble que le plaignant avait été impliqué dans une enquête interne qu'Agriculture Canada avait menée au sujet d'allégations que ses fonctionnaires utilisaient ses véhicules pour fins personnelles. Agriculture Canada avait versé ces renseignements dans le SRRJ; chaque fois que les douaniers inscrivaient le nom du plaignant dans le système au poste-frontière, l'alerte était donnée. Pensant que le plaignant était recherché, on l'envoyait subir un interrogatoire secondaire.

Comme les douaniers ne faisaient que réagir aux renseignements inscrits dans le SRRJ par Agriculture Canada, le point focal de l'enquête a porté sur ce ministère. L'enquêteur a constaté que le nouveau système de surveillance des Douanes avait du simplement dépasser la programmation du SRRJ, qui ne pouvait plus distinguer les données d'application de la loi, dont les douaniers avaient besoin, des autres renseignements dont ils auraient pu se passer.

Loi sur la protection des renseignements personnels. La Loi contrôle la communication des renseignements personnels par l'administration fédérale, mais elle n'empêche pas les ministères et organismes de s'acquitter de leur mandat légal et ne protège pas les personnes qui faisaient leurs déclarations de revenus.

La veuve d'un ancien combattant canadien s'est plainte au Commissariat que Revenu Canada avait révélé son revenu en intérêts aux Programmes de la sécurité du revenu, qui avaient alors réduit son allocation au conjoint au titre des prestations de la sécurité de la vieillesse ainsi que du supplément de revenu garanti. Qui plus est, les Programmes de la sécurité du revenu avaient communiqué ces renseignements à Anciens combattants Canada, qui avait ensuite retiré à la veuve sa pension d'invalidité de guerre.

L'enquête du Commissariat a globalement confirmé les allégations de la plaignante. Les Programmes de la sécurité du revenu n'avaient pas contesté la demande de prestations de l'intéressée. Ils ont pour pratique de vérifier les revenus des demandeurs de prestations de la sécurité de la vieillesse avec Revenu Canada, et ils avaient communiqué les renseignements sur le revenu en intérêts de la plaignante à Anciens combattants Canada. Les deux ministères ont prouvé que la communication était autorisée dans chaque cas par une loi, de sorte qu'elle était conforme à la *Loi sur la protection des renseignements personnels*, qui autorise les institutions gouvernementales à communiquer des renseignements personnels si une autre loi ou un règlement les y autorise.

En l'occurrence, la communication des renseignements par Revenu Canada aux Programmes de la sécurité du revenu est autorisée par l'article 241 de la *Loi de l'impôt sur le revenu*, et celle des Programmes aux Anciens combattants par l'article 33 de la *Loi sur la sécurité de la vieillesse*.

Le Commissaire a jugé la plainte non fondée.

L'enquêteur du Commissariat a téléphoné au SERT. Elle n'avait qu'un NAS, un mois et une année de naissance, mais elle a pu confirmer qu'un certain contribuable reçoit son remboursement de TPS tous les trimestres et quand le remboursement lui est envoyé par la poste, sa limite de déductions au titre des RCEFR pour l'année de déclaration, ainsi que le montant du remboursement d'impôt sur le revenu auquel il a droit.

De toute évidence, les mesures de protection du SERT laissaient à désirer, il fallait les renforcer.

Revenu Canada n'était pas disposé à envisager des changements qui rendraient l'accès au système plus difficile pour les contribuables. Le SERT est un moyen commode et économique de répondre aux questions les plus fréquentes de ces derniers, et plus de deux millions d'appels y ont été placés l'année dernière.

Bref, Revenu Canada a rejeté la proposition du Commissariat d'attribuer un numéro d'identification personnel (NIP) aux contribuables, en disant que ce serait à la fois peu pratique et coûteux, puisqu'attribuer un NIP à chaque contribuable coûterait plus de 4,5 millions de dollars, simplement en frais de poste. Plusieurs autres moyens d'identification supplémentaires ont été envisagés et rejetés, parce qu'ils auraient été trop faciles à deviner ou ne figuraient pas dans la base de données fiscale.

La dernière proposition du Commissariat a permis de résoudre le problème. On demandera à ceux qui téléphonent au SERT de préciser le «revenu total» inscrit à la ligne 150 de leur déclaration de revenus. Il est peu probable que d'autres personnes connaissent ce détail, qui serait difficile à deviner ou à voler.

L'administration fédérale fait des échanges de renseignements sur l'impôt, les revenus et les avantages sociaux

Une autre plainte montre bien que les Canadiennes et les Canadiens doivent comprendre que l'administration fédérale peut communiquer des renseignements qui les concernent sans leur consentement et ce, dans plusieurs circonstances toutes précisées par la

de l'agente a peut-être exacerbé la difficulté. Il est évident que n'importe quelle fonctionnaire considérerait une discussion de son cycle menstruel comme privée, et qu'elle pourrait juger insultant d'être forcée d'en parler.

Après notre enquête (et une autre interne menée par le Centre psychiatrique), les autorités responsables ont publié un ordre permanent informant le personnel des programmes à l'intention des contrevenants autochtones. Le dernier point de ce document, intitulé "Special Gifts of Woman Within Aboriginal Spiritual Beliefs" se lit comme il suit [traduction] :

Pour faire preuve de respect envers les autochtones et pour travailler avec eux, la participation individuelle et la répartition des tâches devraient être volontaires, dans toute la mesure du possible.

Le directeur général du Centre a confirmé qu'aucune fonctionnaire n'a été et n'est tenue d'informer ses superviseurs (ou qui que ce soit d'autre) de son cycle menstruel.

Le Commissaire a conclu qu'il n'y avait pas de preuve que la plainte était fondée.

Il faut protéger le service téléphonique de renseignements fiscaux

Parfois, les gens n'attendent pas que des renseignements personnels soient communiqués à tort pour saisir le Commissariat d'un problème potentiel. On l'a constaté par exemple dans le cas du Service électronique de renseignements par téléphone (SERT) avec lequel les contribuables peuvent communiquer pour obtenir de l'information de base sur leurs déclarations ou sur leurs remboursements.

Le plaignant, un employeur, craignait qu'il pourrait téléphoner au SERT—à l'instar d'autres employeurs, sans doute—pour obtenir des renseignements fiscaux sur ses employés, étant donné qu'il avait l'information nécessaire pour y avoir accès, c'est-à-dire les numéros d'assurance sociale et les dates de naissance de ses employés. C'était de la prescience : un autre plaignant s'était fait voler ses papiers, et quelque'un s'en était servi pour obtenir des renseignements du SERT.

En effet, la Commission doit souvent vérifier les renseignements, par exemple lorsque le revendicateur est malhonnête ou lorsqu'elle soupçonne qu'il a présenté plusieurs fausses revendications du statut de réfugié.

La plainte n'était pas fondée.

Vie privée et croyances spirituelles

Une des plaintes que le Commissariat a reçue cette année laissait entrevoir la possibilité d'une incompatibilité de droits individuels, à savoir le droit à la vie privée des agents du Service correctionnel et les croyances spirituelles des détenus autochtones.

Un député a porté plainte au Commissariat : une de ses comettantes, une agente du Service correctionnel affectée au Centre psychiatrique régional de Saskatoon, s'était fait demander d'informer son superviseur de ses menstruations. Selon l'agente, tout avait commencé quand deux employés de soutien autochtones étaient venus lui parler pendant qu'elle montait la garde lors d'une séance de sudation traditionnelle, à l'occasion de la première visite à l'établissement d'un guérisseur autochtone. Ces employés lui avaient expliqué que, dans les cultures autochtones, la menstruation intensifie les pouvoirs normalement associés à la procréation. Or, les autochtones considèrent comme dangereux pour les hommes et pour les objets sacrés que renferme l'étuve d'être exposés de près à ces pouvoirs accrus.

L'agente avait informé son superviseur de l'incident qui lui aurait alors demandé d'informer le gestionnaire de quart quand elle serait menstruée, afin qu'elle puisse être réaffectée.

L'enquêteure a été incapable de confirmer l'une ou l'autre de ces conversations. Les employés de soutien ont nié avoir abordé le sujet avec l'agente, et le superviseur a nié avoir demandé ce renseignement. Il a déclaré avoir simplement offert à l'agente de la faire relever d'une gestionnaire femme et de la faire affecter à d'autres fonctions, si elle voulait respecter les croyances des autochtones.

Comme les déclarations étaient contradictoires et qu'il n'y avait pas de témoins, l'enquêteure a été bien forcée de conclure que rien ne prouvait l'allégation de l'agente, à savoir que SCC avait tenté d'obtenir de l'information sur ses menstruations. Cela dit, il est bien possible qu'il y ait eu un malentendu, car la réaction quelque peu ambiguë du superviseur

La Commission de l'immigration et du statut de réfugié—besoin des dossiers d'immigration

Le Commissaire a conclu que la LMA autorise la SCHL à obtenir des renseignements suffisants (avec les copies nécessaires) sur les locataires et sur leurs revenus afin de déterminer s'ils sont admissibles à une subvention. La collecte de ces renseignements concilie logiquement le droit individuel des locataires à la vie privée et le droit de la SCHL de s'assurer que l'aide financière qu'elle fournit est justifiée et raisonnable. Bref, les plaintes n'étaient pas fondées.

Un avocat spécialisé en droit de l'immigration a contesté la quantité des renseignements que la Commission de l'immigration et du statut de réfugié peut légalement obtenir de Citoyenneté et Immigration Canada au sujet des revendicateurs du statut de réfugié. Il a aussi contesté les pouvoirs de la Commission d'examiner des renseignements concernant d'autres membres de la famille du revendicateur dans le contexte de son évaluation de la demande.

La Commission a démontré que l'évaluation des revendications du statut de réfugié est un élément du processus global d'immigration et que, par conséquent, la Loi sur l'immigration l'autorise à examiner les renseignements personnels recueillis par Immigration Canada avant de trancher la demande du revendicateur. Il s'ensuit qu'échanger des renseignements compatible avec la raison pour laquelle les renseignements sont recueillis. Ceci est donc conforme aux dispositions de la Loi sur la protection des renseignements personnels, qui interdit la communication de ces renseignements sans le consentement de la personne concernée, à moins qu'ils soient communiqués pour les fins auxquelles ils ont été recueillis ou pour des fins compatibles avec celles-ci.

Le Commissaire a conclu qu'il était raisonnable que la Commission tienne compte des renseignements relatifs aux autres membres de la famille du revendicateur pour évaluer sa demande.

Revenu de locataires communiqués pour l'obtention de logements subventionnés

Deux plaignants ont contesté les raisons pour lesquelles leurs coopératives de logements avaient recueilli et communiqué à la SCHL des renseignements détaillés sur leur revenu afin de prouver qu'ils avaient droit à un logement subventionné.

Les coopératives fournissent un logement aux familles et aux personnes à revenu faible et moyen. Les locataires admissibles paient un pourcentage de leur revenu en guise de loyer; la SCHL paie le reste. De plus, elle contribue à financer l'hypothèque de la coopérative.

Dans un des cas, des membres d'une coopérative de Vancouver ont contesté le droit de la direction de la coopérative de demander des copies des avis de cotisation d'impôt sur le revenu des locataires. Le directeur de la coopérative a justifié sa position en disant que l'entreprise avait besoin de preuves suffisantes du revenu des locataires pour justifier que la SCHL subventionne leurs logements. Comme on doutait que certains des locataires déclarent leurs véritables revenus, il estimait que les avis de cotisation étaient la façon la plus prudente et la plus raisonnable de les vérifier.

Dans le deuxième cas, le plaignant a déclaré que, lors d'une vérification d'une coopérative de logements de Scarborough, en Ontario, les vérificateurs de la SCHL avaient mis la main sur une liste complète de tous les locataires qui devaient un arriéré de loyer, y compris le montant des arriérés, de même qu'un imprimé des paiements de loyer versés par tous les locataires.

La SCHL conclut des ententes avec des groupes sans but lucratif pour subventionner des logements—loués sans but lucratif—en vertu de la *Loi nationale sur l'habitation (LNA)* et de son règlement. Ces ententes obligent les coopératives à obtenir des renseignements sur la situation financière des locataires bénéficiant d'un logement subventionné, afin de justifier le versement de la subvention par la SCHL, et de conserver des preuves suffisantes pour faciliter les vérifications, par a SCHL, des subventions dont bénéficient les locataires.

concernant. Or, le sous-traitant a refusé, afin de protéger l'identité des témoins.

Le Commissaire était disposé à poursuivre l'affaire, puisqu'il considère la plainte comme fondée, mais l'intéressée a préféré en rester là. Néanmoins, le Commissaire compte bien poursuivre ses démarches à l'égard de plusieurs autres plaintes en instance, notamment contre le MDN, pour que les documents des sous-traitants soient communiqués aux plaignants.

Elections Canada met fin à l'utilisation des numéros de service militaire

Deux membres des Forces armées canadiennes se sont opposés à l'inclusion de leurs numéros de service militaire dans des listes d'envois postaux utilisées par des candidats aux élections fédérales de 1993. Ils avaient tous deux constaté que leur numéro de service militaire figurait dans l'étiquette-adresse apposée sur les documents de campagne d'un de leurs candidats locaux.

L'enquêteur du Commissariat a découvert que le MDN avait en vertu de la *Loi électorale du Canada* fourni à Elections Canada le nom, le numéro de service militaire et l'adresse postale de tous les membres admissibles des Forces. Les militaires ont le choix d'être inscrits sur les listes électorales soit à leur lieu de résidence permanent (souvent là où ils se sont enrôlés), soit à leur adresse postale courante. Ensuite, le directeur général des élections doit fournir ce renseignement au directeur de scrutin de la circonscription correspondant à l'adresse choisie par le militaire pour que l'information puisse être communiquée aux candidats, à leur demande.

Comme la loi précise clairement que le MDN peut communiquer les numéros de service militaire à Elections Canada et que cet organisme peut les communiquer aux candidats, la plainte n'est pas fondée. Toutefois, le Commissaire craignait que communiquer les numéros porte atteinte à la vie privée des intéressés, étant donné qu'Elections Canada a reconnu ne pas en avoir absolument besoin. Par suite de la plainte, Elections Canada a convenu de réclamer une modification de la *Loi électorale du Canada* afin d'éliminer l'obligation, pour le MDN, de lui fournir ces numéros. La modification réclamée fera

Sous-traitant qui refuse de transmettre ses dossiers

Troisièmement, dans les deux cas, les renseignements personnels ne faisaient pas encore partie du domaine public. Si les agents du détachement local avaient attendu jusqu'à ce que des accusations soient portées contre les intéressés, la communication des renseignements personnels aurait alors pu être autorisée.

Dans ses derniers rapports annuels, le Commissaire a rappelé aux ministères de ne pas se décharger sur leurs sous-traitants de leurs responsabilités en matière de protection des renseignements personnels. En effet, le sous-traitant est tout simplement un agent du ministère. Tous les renseignements personnels qu'il obtient — ou prépare — appartiennent au ministère, de sorte qu'ils sont protégés par la *Loi sur la protection des renseignements personnels*. Cela signifie que la personne concernée doit y avoir accès, qu'ils ne doivent pas être communiqués sans autorisation, que le sous-traitant doit les mettre à la disposition du ministère pour fins de vérification de l'exécution du marché qui les lie, et que les critères de conservation et de retrait des renseignements doivent être respectés à l'expiration du marché.

Pourtant, malgré des avertissements répétés, il est toujours difficile pour les demandeurs d'avoir accès aux renseignements personnels recueillis à contrat.

Par exemple, une dame a récemment demandé au Commissariat de l'aider à obtenir les pièces justificatives recueillies par un sous-traitant que le ministère de la Défense nationale (MDN) avait chargé d'enquêter sur sa plainte de harcèlement sexuel. Bien que le MDN ait remis à la dame un exemplaire du rapport final, ce document ne contenait ni la liste des témoins interrogés, ni les questions posées non plus que les réponses.

L'enquêteur du Commissariat a constaté que le MDN n'avait pas ces pièces justificatives. Il lui a donc demandé d'enjoindre au sous-traitant de les lui remettre, afin de pouvoir s'acquitter de son obligation de faire en sorte que la plaignante ait accès aux renseignements la

GRC—Communication injustifiée de l'arrestation d'employés

Trois personnes se sont plaintes que la GRC ait communiqué à tort leur arrestation à leurs employeurs.

Dans le premier cas, un agent de la GRC avait communiqué des détails sur l'arrestation de l'intéressé au pénitencier de Matsqui, où ce dernier travaillait. Dans le second cas, un autre agent de la GRC avait informé un directeur de banque que deux de ses employés avaient été arrêtés pour vol à l'étalage.

La GRC a défendu les actes de ses agents en disant qu'il était d'intérêt public de veiller à ce que les employés soient informés de l'arrestation des employés en cause et des accusations qui allaient être portées contre eux. Selon la GRC, la cote de sécurité de l'employé du Service correctionnel aurait pu devoir être modifiée en conséquence, et il était possible que les employés de la banque aient occupé des postes de confiance.

Néanmoins, le Commissaire a considéré les plaintes comme fondées, pour plusieurs raisons.

Premièrement, la GRC n'avait pas respecté la procédure applicable à la communication de renseignements personnels pour raisons d'intérêt public établie dans la *Loi sur la protection des renseignements personnels*. Seule la haute direction d'un organisme devrait décider de communiquer des renseignements personnels pour de telles raisons, et encore, seulement après avoir déterminé si ces raisons «justifieraient nettement» une éventuelle violation de la vie privée des personnes intéressées. En outre, l'administration fédérale est tenue d'aviser le Commissaire de la communication imminente des renseignements afin qu'il puisse décider d'informer ou pas la personne concernée, s'il le juge bon.

Deuxièmement, la GRC a sa propre procédure pour informer les employeurs que les actes de leurs employés risquent d'avoir sapé leur fiabilité, et elle ne l'a pas suivie. En effet, les agents du détachement local ont décidé d'agir sans avoir obtenu l'autorisation des hauts grades de l'administration centrale, qui sont seuls habilités à prendre ces décisions-là.

personnels la concernant sur l'emploi, la paye, les présences, les griefs, les questions de SST&E et les activités de surveillance. Postes Canada n'avait pas consulté ces documents en réponse à la demande de communication des renseignements que la plaignante avait présentée en vertu de la *Loi sur la protection des renseignements personnels*, parce que le gestionnaire concerné soutenait que ces dossiers lui appartenaient personnellement. À la toute fin, Postes Canada a obtenu les dossiers du gestionnaire et en a fait parvenir une copie à la plaignante.

D'autres plaintes de cette même personne ont été jugées justifiées et concernaient la façon de Postes Canada de traiter ses renseignements personnels, notamment en recueillant des renseignements médicaux de SST&E directement de son orthopédiste sans avoir obtenu son consentement, et en n'ayant pas retiré des documents disciplinaires de son dossier d'emploi, en dépit des instructions expresses à cet égard dans les décisions arbitrales ainsi que dans les arbitrages de griefs.

À l'administration centrale de Postes Canada on a reconnu que les gestionnaires gardaient leurs propres dossiers du personnel parce qu'ils le jugeaient pratique, mais ils ont déclaré ignorer que la Division Huron se livrait à des activités de surveillance. Ils ont mis fin à ces abus : les employés en cause ont écopé de sanctions disciplinaires, voire ont été démis de leurs fonctions, quand ils n'ont pas démissionné. Postes Canada a écrit à la plaignante afin de lui présenter des excuses pour les activités de surveillance dont elle avait fait l'objet et lui a donné l'accès qu'elle réclamait à tous ses documents.

Bien qu'il n'existe qu'un seul dossier "officiel" par employé, bien des gestionnaires de Postes Canada conservent dans leur bureau leurs propres dossiers sur leurs employés, à des fins administratives. L'organisme néglige fréquemment d'inclure ces derniers dossiers dans ses réponses aux demandes d'accès qu'il reçoit des employés, négligence qui suscite de nombreuses plaintes—et rappels—auprès du Commissariat. Bien que les dossiers des gestionnaires devraient logiquement ressembler aux dossiers officiels, les employés devraient toujours spécifier que leurs demandes d'accès visent l'ensemble des renseignements détenus par l'organisme, y compris les dossiers de leurs gestionnaires.

Des 15 plaintes déposées par la plaignante, toutes sauf deux ont été jugées fondées.

faire surveiller en dehors de ses heures de travail. Leur demande avait été rejetée.

Frustrés, ces gestionnaires ont retenu les services d'un ancien inspecteur des Postes pour la surveillance non seulement de la plaignante, mais aussi deux autres employés. Bien que les responsables du service de sécurité des Postes aient nié toute participation à ces agissements, l'enquêteur a découvert que l'un d'entre eux connaissait l'ancien inspecteur des Postes et qu'il l'avait recommandé à la direction pour assurer la surveillance voulue.

Les gestionnaires ont donc embauché le détective (sous d'autres fonctions postales) pour suivre et photographier la plaignante pendant son congé de maladie dans l'espoir de prouver que sa blessure au dos n'était pas réelle. Quand la surveillance n'a rien donné, ils ont détruit ce qu'ils croyaient être la plus grande partie des pièces compromettantes. Néanmoins, l'enquêteur du Commissariat a trouvé des photocopies des photographies de surveillance dans la partie des accidents du travail du dossier de santé et de sécurité au travail et d'environnement (SST&E) de la plaignante.

Le personnel des services de SST&E a nié toute connaissance des activités de surveillance et n'a pas pu dire comment les photographies s'étaient retrouvées dans le dossier. Elles n'y étaient certainement pas six mois auparavant, lorsque l'intéressée avait eu accès à ce qu'elle croyait être tous ses renseignements personnels.

L'enquêteur a constaté que la direction n'avait pas laissé la plaignante consulter les 165 pages de la partie des soins de santé de son dossier de SST&E. Postes Canada a prétendu qu'il s'agissait d'une omission par inadvertance. Or, cette partie du dossier contenait la plupart des allusions aux activités de surveillance.

Ensuite, Postes Canada a tenté de persister dans son refus de communiquer les renseignements sur les activités de surveillance contenus dans le dossier prétendant que leur divulgation nuirait au déroulement d'une enquête licite, c'est-à-dire en invoquant l'alinéa 22(1)b) de la Loi. Le Commissaire a rejeté cette prétention.

Qui plus est, l'enquêteur a constaté que le gestionnaire de la Division Huron, de qui la plaignante relevait, avait en sa possession trois gros volumes—totalisant plus de 750 pages—de renseignements

personnels qui les concernent seront conservés indéfiniment et qu'ils seront cédés un jour aux Archives nationales. Il faut que les Canadiens sachent pourquoi les renseignements sont recueillis, comment ils seront utilisés, combien de temps ils seront conservés et à qui ils seront communiqués. Ces principes sont absolument fondamentaux pour l'application de la *Loi sur la protection des renseignements personnels*, et il faut absolument que la banque de données personnelles la plus importante de l'État les respecte.

Dépersonnaliser les données du recensement est le facteur critique si l'on veut obtenir l'entière collaboration des citoyens au recensement et apaiser une fois pour toutes les craintes qu'ils expriment encore et toujours à cet égard.

Détective privé et dossiers "secrets" à Postes Canada

Les allégations d'une facteure qui reprochait à Postes Canada d'avoir recueilli et communiqué des renseignements personnels de nature médicale à son sujet (et par la suite refusé de lui y donner accès) étaient déjà suffisamment graves, mais l'enquête du Commissariat a révélé que ce n'était que la pointe de l'iceberg.

En effet, en vérifiant les dossiers l'enquêteur a constaté que des gestionnaires de la Division Huron avaient retenu les services d'un détective privé pour effectuer la surveillance de l'employée. Notre enquêteur a aussi constaté l'existence d'un classeur rempli de dossiers «secrets» que le gestionnaire maintenait sur ses employés, et qu'il considèrerait comme sa propriété privée, échappant ainsi à l'application de la *Loi sur la protection des renseignements personnels*.

La plaignante avait fait une chute et s'était blessée au dos en livrant le courrier et avait réclamé une indemnité pour lésion professionnelle. Même si elle avait subi une intervention chirurgicale au dos, qu'elle devait en subir une seconde, que son chirurgien et les médecins retenus par Postes Canada étaient d'accord sur la cause et la gravité de ses blessures, les gestionnaires contestaient sa demande d'indemnité. À leur avis, les blessures de la plaignante avaient été causées par des accidents de la route antérieurs plutôt que par sa chute. Ils avaient demandé au service de sécurité des Postes l'autorisation de la

La destruction de l'information—Solution optimale pour la protection de la vie privée

- modifier les procédures de contrôle et de suivi afin de minimiser le fardeau imposé aux répondants;
- prévoir une infoigne du recensement; et
- mettre à l'essai un système de contrôle centralisé.

La procédure actuelle consiste à conserver sur microfilm des copies des questionnaires du recensement et de tous les autres documents permettant de relier les réponses à des personnes identifiables; cette procédure a un impact majeur sur la protection à long terme de la vie privée des Canadiens et des Canadiennes.

La Loi sur la statistique interdit absolument à Statistique Canada de communiquer à quiconque, pour quelle que raison que ce soit, des renseignements personnels tirés du recensement. Les documents des recensements réalisés jusqu'à 1901 inclusivement sont conservés aux Archives nationales, et le public y a accès pour fins de recherche. Par contre, les documents des recensements réalisés depuis sont conservés par Statistique Canada, et personne, sauf le personnel de cet organisme—pas même l'Archiviste national—n'y a accès.

La façon optimale d'assurer la protection de la vie privée des Canadiens consisterait à détruire tous les documents personnalisés du recensement de 1991 (ainsi que tous les autres documents du recensement qui ne font pas déjà partie du domaine public), une fois que Statistique Canada aura traité les données pour s'assurer de leur qualité et de leur exactitude. À cette fin, il faudrait que Statistique Canada obtienne une modification des délais de conservation et de retrait des documents du recensement approuvés par l'Archiviste national en vertu de la *Loi sur les archives nationales du Canada*.

Or, si Statistique Canada est disposé à détruire les documents du recensement de 1991, la direction des Archives nationales se montre extrêmement réticente. Il faudra du temps pour surmonter cet obstacle. Cela dit, si les Archives nationales empêchent Statistique Canada de détruire les données personnalisées du recensement, le Statisticien en chef doit informer les Canadiens que les renseignements

Si le projet pilote donne de bons résultats, Statistique Canada compte employer cette méthode à l'échelle nationale pour le recensement de 2001.

D'autres plaignants se sont opposés au fait de devoir partager un questionnaire avec d'autres membres du ménage. Selon eux, cela les forçait à divulguer les renseignements à des personnes qui pouvaient ne pas leur être apparentées. Si Statistique Canada ne distribuait qu'un formulaire par ménage, c'est pour réduire au minimum ses frais de collecte et de traitement. Toutefois, même si la plupart des ménages n'ont pas besoin de plusieurs questionnaires et qu'ils crieraient probablement au gaspillage s'il fallait qu'on leur en remette plus d'un, Statistique Canada va offrir de remettre un questionnaire individuel à qui le demandera.

Bref, le Commissariat a persuadé Statistique Canada d'apporter plusieurs changements d'importance à ses procédures de recensement, afin de minimiser son intrusion dans la vie privée des Canadiennes et Canadiens, à savoir :

- éliminer certaines des questions des deux versions du questionnaire;
- simplifier le questionnaire et son guide, pour que les répondants comprennent mieux les questions et leur raison d'être;
- affecter dans toutes la mesure du possible les recenseurs à des voisinages où ils ne sont pas susceptibles d'être connus;
- offrir aux répondants la possibilité d'envoyer leur questionnaire rempli par la poste à un bureau régional, afin que les recenseurs locaux ne puissent pas lire leurs réponses;
- expliquer clairement le rôle des recenseurs locaux dans la documentation distribuée avec le questionnaire;
- former le personnel du recensement pour le sensibiliser à respecter rigoureusement les principes de confidentialité et de protection de la vie privée dans toutes les phases du recensement;

Par conséquent, Statistique Canada va devoir maintenir cette pratique, mais en s'engageant à expliquer clairement le rôle des recenseurs sur les enveloppes que les répondants doivent remettre personnellement et par la poste. Ainsi, ceux qui ne voudraient pas que le recenseur local puisse lire leurs réponses pourront s'arranger pour que quelqu'un d'autre vienne recueillir leur questionnaire, ou le renvoyer par la poste au bureau régional le plus proche.

Le fait que les commissaires et autres recenseurs sont autorisés à travailler chez eux inquiétait aussi plusieurs plaignants : l'idée que leur formulaire dûment rempli se retrouverait sur la table de cuisine de ces gens-là leur faisait sérieusement douter de la confidentialité des procédures de collecte. Or, Statistique Canada donne des instructions précises au personnel du recensement afin d'assurer la confidentialité des renseignements collectés et affirme que tous ses représentants sont parfaitement sensibilisés à leurs responsabilités de protection des données.

Projet de contrôle centralisé

Statistique Canada compte réaliser à l'occasion du recensement de 1996 un important projet pilote qui pourrait lui permettre d'éliminer une grande partie des irritants de ses procédures de collecte. Dans la zone du projet, qui englobe 400 000 personnes dans dix circonscriptions électorales de la région d'Ottawa, tous les questionnaires du recensement seront envoyés directement par la poste aux répondants, qui les renverront eux aussi par la poste, après les avoir remplis, aux bureaux de district plutôt qu'au recenseur local.

Cette méthode éliminera la distribution des questionnaires de porte-à-porte, la nécessité d'avoir recours à des recenseurs et, par conséquent, le risque que des voisins lisent les questionnaires remplis, ainsi que les craintes pour la protection des données passant par le domicile des recenseurs.

Lorsque le personnel du bureau de district sera incapable de résoudre par téléphone les problèmes attribuables à des questionnaires manquants ou incomplets, on fera appel à des agents itinérants venus d'ailleurs. Cela devrait réduire nettement le risque que les formulaires soient traités par des recenseurs que les répondants connaissent.

limitera à poser des questions pour obtenir l'information démographique de base.

Comme le Commissaire lui a fait savoir que la justification de nombreuses questions n'était pas claire, Statistique Canada va aussi modifier le Guide, afin qu'il soit plus facile à lire et qu'il explique mieux pourquoi l'on demande l'information et comment on s'en servira. De plus, on prévoira pour le recensement une infoligne téléphonique pour répondre aux questions du public en matière de confidentialité et de protection de la vie privée, ainsi que pour l'aider à remplir les questionnaires.

Protection des procédures de collecte

Pour apaiser les craintes des plaignants qui disaient que les procédures de collecte menaçaient l'intimité des répondants, les enquêteurs ont étudié le serment d'office des recenseurs ainsi que leurs méthodes d'embauche et de formation de même que celles de la collecte et du traitement des données.

Les procédures du recensement de 1991 semblaient poser des risques pour la protection des données. La formation que Statistique Canada fournissait aux recenseurs n'insistait pas suffisamment sur les principes de protection des renseignements personnels ni sur les plaintes croissantes du public à cet égard. Pour y remédier, Statistique Canada a accepté d'accorder plus d'importance à ces facteurs dans son programme de formation en vue du prochain recensement.

Par ailleurs, de nombreux plaignants avaient dit craindre que des voisins travaillant comme recenseurs prennent connaissance des questionnaires qu'ils avaient remplis. Ces plaignants étaient partis du principe que leurs réponses seraient lues par un bureaucrate anonyme de l'administration centrale de Statistique Canada, à Ottawa, et non par quelqu'un qu'ils connaissaient.

Statistique Canada va s'efforcer de réduire les risques que les recenseurs recueillent de l'information d'une personne qu'ils connaissent, en les affectant à un autre secteur de recensement que celui de leur voisinage. Malheureusement, cela risque d'être difficile dans les régions rurales, où la meilleure façon de s'assurer que tous les ménages sont recensés consiste à affecter au secteur un recenseur qui le connaît parfaitement.

Questions « intrusives »

La plupart des plaignants se sont opposés à ce qu'on leur pose des questions sur leur origine ethnique, leur religion, leur fécondité, leur logement, leur santé physique et mentale ou sur le nombre « de personnes ayant un domicile habituel ailleurs au Canada » qui avaient passé la nuit chez eux. Une dame qui recevait des soins psychiatriques avait été si perturbée par la question sur sa santé mentale et physique que son mari a déchiré le formulaire. D'autres plaignants ont soutenu que toutes les questions destinées à autre chose qu'à déterminer le nombre de personnes dans la maison dépassaient la définition de recensement, de sorte que rien ne les obligeait à y répondre.

La recherche a révélé que le recensement est plus qu'un simple dénombrement des habitants du pays, et ce, depuis près d'un siècle. Les données du recensement sont utilisées pour calculer les paiements de transfert aux provinces, évaluer le changement économique et social ainsi que prévoir les besoins d'écoles, de services médicaux et d'autoroutes de la société canadienne. En outre, Statistique Canada vend des données globales (dépouillées des identifications personnelles et combinées avec celles d'un nombre minimum d'autres personnes) sur divers supports électroniques, notamment sur CD-ROM, sur disquette et sur bande magnétique, en plus de faire des essais afin d'y donner éventuellement accès sur Internet.

Néanmoins, certains considèrent les questions comme intrusives, surtout s'ils font partie du cinquième de la population qui reçoit le formulaire complet. Cela soulève de sérieuses questions de protection de la vie privée, en raison du caractère personnel des renseignements demandés, de la possibilité de les relier aux individus et du fait qu'ils sont conservés indéfiniment.

Le Commissariat a donc entrepris un long processus de consultation avec Statistique Canada; les deux parties tenaient à surmonter les problèmes de protection de la vie privée sans rendre le recensement lui-même impossible. Afin de réduire les intrusions, il n'y aura dans ni l'une ni l'autre des versions du questionnaire du recensement de 1996 de question sur les personnes vivant ailleurs ayant passé la nuit chez les répondants. Les questions sur la religion et la fécondité seront éliminées de la version complète du formulaire, et les deux questions sur le logement du répondant seront amputées de la version abrégée, qui se

Même le recensement doit respecter la vie privée

Le Commissariat a mené à bien cette année l'enquête la plus longue et la plus laborieuse de son histoire sur les 33 plaintes qu'il avait reçues au sujet du dernier recensement. Et le travail en valait vraiment la peine, car il a incité Statistique Canada à apporter d'importantes modifications aux préparatifs du prochain recensement, prévu pour 1996. Le recensement est la plus importante, la plus coûteuse et potentiellement aussi la plus intrusive des activités de collecte de renseignements personnels de l'administration fédérale. Toutefois, bien des gens diraient aussi que c'est la plus utile pour la société et pour l'économie canadiennes.

En l'occurrence, le défi consiste à concilier l'importance du recensement pour l'État et le caractère intrusif inhérent à tout questionnaire. Comment une démocratie peut-elle concilier son besoin d'obtenir des données fiables et sa saine réticence à obliger les citoyens à lui fournir des renseignements détaillés sur leur origine ethnique, leur religion, leur style de vie et leur santé, en sachant que les données recueillies ne seront jamais détruites?

C'est une question d'une envergure telle qu'elle dépasse même celle du mandat d'un commissaire à la protection de la vie privée, et qui devrait peut-être faire l'objet d'un débat de société. Quoi qu'il en soit, les enquêteurs du Commissariat se sont concentrés sur la collecte, l'utilisation, la conservation et la communication des renseignements personnels des Canadiennes et Canadiens. Pour se préparer à l'enquête, ils ont étudié l'histoire du recensement et sa justification, ainsi que les utilisations des données recueillies, de même que les pratiques comparables d'autres pays. Ensuite, ils ont tenté de trancher les 26 plaintes qui leur restaient (les sept autres avaient été jugées non fondées, ou retirées).

Globalement, il y avait deux types de plaintes, celles qui contestaient le caractère intrusif de certaines des questions et celles où l'on alléguait que les procédures de collecte de Statistique Canada sapaient ses garanties de confidentialité.

Plaintes "résolues"

Quoique le processus d'accès informel est louable, le détenu devrait se voir offrir le choix. Les institutions ne devraient pas mettre de l'avant un système qui oblige une personne à renoncer à ses droits en vertu de la Loi à la seule fin de hâter le processus. Certains détenus choisiront la voie formelle en vertu de la Loi, soit par ce qu'ils n'ont pas confiance en l'institution ou encore parce qu'ils désirent conserver leur droit de recours à un enquêteur indépendant.

Les habitudes du Rapport annuel remarqueront sûrement notre nouvelle catégorie de ventilation des plaintes : le Commissaire en considère plusieurs comme résolues. Dans le passé, le Commissaire se creusait la cervelle pour classer les plaintes qu'il aurait été trop rigide de considérer comme « fondées », puisqu'elles résultaient essentiellement d'un problème de communication ou d'un malentendu. Le pouvoir de l'ombudsman repose sur la souplesse qu'il lui permet de résoudre les problèmes; c'est pour ainsi dire sa spécialité. Nous appelons plaintes résolues celles où

■ il y a eu malentendu ou manque de communication entre le plaignant et le ministère au sujet de la nature des renseignements demandés, et où les deux parties ont accepté une solution qui les satisfait toutes deux;

■ le plaignant a déclaré que des renseignements précis faisaient défaut, alors que le ministère a maintenu qu'il avait communiqué les documents, tout en acceptant sans se faire prier de les communiquer de nouveau;

■ le ministère avait le droit de se prévaloir d'une exception pour ne pas communiquer les renseignements, mais a été persuadé par l'enquêteur du Commissariat de se prévaloir de son pouvoir discrétionnaire pour les communiquer;

■ l'enquête a révélé un manque d'uniformité dans le traitement d'un gros volume de renseignements pour le demandeur, et le ministère a consenti à lui communiquer plus de renseignements, par souci d'uniformité.

Les exemples suivants sont tirés des 1 307 plaintes réglées au cours de l'année écoulée.

à une institution gouvernementale assujettie à la Loi. Certains des contrats liant les deux parties excluent spécifiquement l'obligation de fournir les déclarations ou témoignages recueillis pendant l'enquête, et n'exigent des consultants que le rapport final. Il y a également eu des cas dans lesquels les consultants ont tout simplement refusé de divulguer le moindre renseignement au ministère sous le prétexte que les témoins avaient été assurés de la confidentialité de leurs interventions. Légalement, il faut alors se demander qui «contrôle» les documents.

Il y a eu des progrès. Dans le contexte d'une plainte analogue portée cette année contre Travaux publics et Services gouvernementaux Canada, le sous-ministre a reconnu que les notes du sous-traitant relevaient non pas de celui-ci, mais bien du ministère, de sorte qu'elles devraient être communiquées aux personnes qui les réclament en vertu de la *Loi sur la protection des renseignements personnels*.

Accès officiel versus officiieux

Un point soulevé avec Service correctionnel Canada cette année visait la façon dont les détenus avaient accès à leurs renseignements personnels.

En vertu de la *Loi sur la protection des renseignements personnels*, les détenus jouissent du droit d'accès et de correction de leurs renseignements personnels, de même que le droit de porter plainte auprès du Commissaire à la protection de la vie privée et en dernier recours auprès de la Cour fédérale s'ils croient en avoir été lésés. Cependant pour se prévaloir de ce recours, les détenus doivent d'abord remplir une demande d'accès en vertu de la Loi. Service correctionnel Canada traite les demandes d'accès à la Direction de l'ALPRP, au Siège social.

Néanmoins une autre avenue s'offre aux détenus. La *Loi sur le système correctionnel et la mise en liberté sous condition* leur confère également des droits informels d'accès et de correction aux renseignements détenus par le SCC. Globalement, le SCC encourage les demandes informelles non seulement parce qu'elles sont traitées directement par l'institution mais encore parce que le processus se déroule plus rapidement. Un membre du personnel est sélectionné dans chaque institution en vue d'aider les détenus à rédiger leur demande. Cependant, ce faisant, les détenus n'ont aucun recours à un enquêteur indépendant.

Enquêtes de plaintes

Après le répit de l'an dernier, les plaintes ont repris de plus belle; cette année, le Commissariat en a reçu le nombre record de 1 783, soit 493 (38 p. 100) de plus que les 1 290 de 1993-1994. Le personnel mené à bien 1 307 enquêtes; il a constaté que 595 des plaintes étaient fondées alors que 645 ne l'étaient pas; 26 des plaintes ont été résolues, et les 41 restantes ont été abandonnées, à la demande du plaignant dans certains cas.

Cette augmentation du nombre de plaintes est en partie attribuable à une augmentation de 78 p. 100 des plaintes découlant d'une prorogation des délais, laquelle résultait dans bien des cas des compressions d'effectif et de la réorganisation de l'administration fédérale. En outre, le quart de ces 729 plaintes a été porté par quatre personnes contre le ministère de la Défense nationale, Revenu Canada et Service correctionnel Canada.

Cette année encore, les plaintes de délais et celles pour refus d'accès à l'information constituent la majorité des plaintes reçues. Néanmoins, les plaintes contestant la collecte, la conservation, l'utilisation et la communication de renseignements personnels (autrement dit celles qui protestent contre une violation de la vie privée) ont connu une importante augmentation (22 p. 100); elles sont passées en 1994-1995 à 348, dont 66 p. 100 relatives à une utilisation ou une communication injustifiée, 20 p. 100 à une collecte abusive et 14 p. 100 à une conservation induisant des renseignements. Il est plus compliqué d'enquêter sur les plaintes contestant l'utilisation et la conservation des renseignements, car les enquêteurs doivent souvent se déplacer, ce qui prolonge d'autant le délai de traitement de la plainte.

Mise à jour sur la sous-traitance

Dans le rapport de l'an dernier, le Commissaire a déploré que certains se voient refuser leurs droits à la vie privée quand les ministères ont recours à la sous-traitance, comme dans l'affaire qui avait inspiré ces réflexions au Commissaire, soient les enquêtes sur le harcèlement.

En l'occurrence, il s'agissait de l'accès aux documents réunis par une personne ou une entreprise non assujettie à la Loi sur la protection des renseignements personnels, mais fournissant des services

Du domaine public?

En l'occurrence, on allègue que les renseignements devraient être communiqués parce que le public y a déjà accès, étant donné qu'il pourrait trouver les noms des anciens députés dans des documents publics, par exemple dans le Guide ou dans le Répertoire parlementaire canadien. Ce dernier contient une liste des députés élus pour chaque circonscription pour toutes les élections qui ont eu lieu depuis la Confédération—ou la création de la circonscription—jusqu'en 1988. Autrement dit, il est très simple pour le lecteur de savoir quels députés ont siégé au moins six ans et sont donc éligibles à une pension.

Toutefois, cela signifie simplement que ces députés ont droit à une pension, pas qu'ils en touchent une. Les variables (option de rachat, remboursement des contributions pour les périodes d'interruption du service en Chambre, mention de centaines de députés décédés depuis) sont assez nombreuses pour rendre les données publiques incomplètes.

Cela dit, plusieurs questions restent sans réponse. Si le public a accès aux renseignements, pourquoi s'est-on adressé à la Cour et pourquoi tout ceci est-il nécessaire? En quoi la communication des seuls noms satisferait-elle le requérant? Pourquoi semble-t-il exister plusieurs versions de la «bonne» liste? Pourquoi TPSGC devrait-il être contraint à communiquer une liste particulière de pensionnés, puisque le public a accès à une liste générale des noms des anciens députés? Quand les noms des survivants (conjointes et personnes à charge) sont retirés de la liste, est-elle encore exacte et complète?

Enfin, comment le fait de savoir quels anciens députés touchent une pension aide-t-il le public à juger de la validité de leur régime de pension, alors que tous les renseignements nécessaires pour évaluer ce régime (la ventilation des contributions des députés et de l'administration fédérale, les intérêts, les débours, les allocations de retrait et les soldes du compte) sont déjà accessibles à qui le veut?

Le ministère a rejeté les recommandations du Commissaire à l'information, de sorte que la Cour fédérale a été saisie de l'affaire.

versée pour chacun et une ventilation des contributions des députés et de l'administration gouvernementale, en application de la Loi sur les allocations de retraite des parlementaires, au 1^{er} septembre 1993.

Le ministère a rejeté la demande en disant qu'il s'agissait là de renseignements personnels exemptés en vertu de la Loi sur l'accès à l'information (sauf quelques cas bien précis). L'intéressé a porté plainte au Commissaire à l'information, qui s'est rangé du côté de TPSGC, à une exception près, celle de la liste des noms des anciens députés. En effet, comme ces noms et la durée du mandat des intéressés figurent dans des documents publics, le Commissaire à l'information a recommandé que TPSGC communique les noms des anciens députés fédéraux qui touchent une pension à ce titre. TPSGC a alors demandé l'avis du Commissariat à la protection de la vie privée.

Le rôle du Commissaire à la protection de la vie privée n'est pas d'aviser les ministères quand divulguer des renseignements personnels. La Loi établit clairement que c'est là la responsabilité du chef de l'organisme qui connaît en profondeur les fichiers et qui doit répondre de leur sécurité. Le Commissaire établit simplement les facteurs à considérer avant de communiquer des renseignements personnels. Les ministères peuvent:

■ chercher à obtenir le consentement à la divulgation des personnes concernées;

■ déterminer si l'intérêt public justifie une quelconque atteinte à la vie privée; ou

■ conclure que les renseignements sont du domaine public.

Le ministère a demandé aux prestataires de consentir à la communication des renseignements, mais beaucoup d'entre eux ont refusé. Le ministère n'estimait pas que l'intérêt public l'emportait suffisamment sur le droit à la vie privée des personnes intéressées, et ne s'est pas prévalu de son pouvoir discrétionnaire de communiquer les renseignements demandés.

comme dans ce cas-là). Le Conseil a refusé de traiter ces notes en vertu de la *Loi sur la protection des renseignements personnels*, estimant que celles-ci appartenaient aux arbitres. Les notes des arbitres ne sont pas conservées dans les dossiers du CCRT et le Conseil estime conséquemment qu'elles ne sont pas sous son "contrôle".

Le Commissaire estime que les notes ont été prises dans le cadre d'un processus administratif. Elles ne sont donc pas la propriété personnelle des membres du conseil puisqu'elles ont été préparées en vue de les aider à remplir leurs fonctions; ce faisant, elles sont donc sous la juridiction du CCRT. La *Loi sur la protection des renseignements personnels* donne à chacun le droit de savoir quels renseignements sont détenus à son sujet par les organismes qu'elle réglemente.

Dans sa demande à la Cour, le Commissaire requiert qu'elle ordonne au CCRT de traiter les notes à la lumière de la *Loi sur la protection des renseignements personnels* et d'accorder au plaignant accès à ceux de ses renseignements personnels auxquels il a droit.

C'est à l'automne prochain que la cause sera entendue.

Consulter le Commissaire—Pensions des députés fédéraux

Des représentants des ministères et organismes téléphonent souvent au Commissariat pour savoir comment concilier le droit collectif du public de savoir et le droit individuel à la vie privée. Une affaire récente montre bien à quel point il faut se méfier des apparences.

Faut-il laisser les faits saper un bon éditorial?

Le débat politique sur ce que d'aucuns prétendent être les pensions farariniennes des députés fédéraux fait toujours rage, et la Cour d'appel fédérale est à revoir un refus d'accès à des renseignements connexes par un ministre. C'est un terrain miné, mais certains commentaires s'imposent quand même.

Afin de poursuivre ce grand débat sur les pensions des députés, quelqu'un avait demandé à Travaux publics et Services gouvernementaux Canada (TPSGC) de lui fournir une liste des noms des prestataires actuels et de ceux des survivants, avec la somme totale

Le ministre des Finances en a appelé de ce jugement à la Cour d'appel fédérale.

Le juge en chef de la Cour d'appel a infirmé le jugement du juge Cullen. La Cour a clairement souligné que les deux lois devaient jouer d'un même statut. Les deux doivent être lues ensemble puisque l'article 19 de la *Loi sur l'accès à l'information* incorpore par référence certains articles de la *Loi sur la protection des renseignements personnels*. Rien ne suggère dans le libellé de ces lois que l'une est subordonnée à l'autre. Elles sont complémentaires et doivent être interprétées harmonieusement de façon à rencontrer les objectifs du législateur.

Quant au test de la caractéristique prédominante, la Cour l'a rejeté, estimant que cette interprétation reviendrait à modifier de façon injustifiée l'article 3 de la *Loi sur la protection des renseignements personnels*. Le juge en chef précise que cet article doit recevoir une interprétation large, illustre qu'il est de neuf catégories ou exemples de renseignements personnels et de quatre catégories d'exceptions. En fait, les renseignements sont ou ne sont pas personnels et il ne saurait y avoir d'autre catégorie de renseignements dont les caractéristiques seraient à prédominance personnelle ou non personnelle. La question de savoir si un employé se trouve à un endroit à un moment précis constitue des renseignements personnels de cet employé.

On refuse accès à des notes—cas devant les tribunaux

Le Commissaire à la protection de la vie privée a porté une deuxième cause devant la Cour fédérale (la première a été évitée à la dernière minute). Le Commissaire a demandé à la Cour fédérale de se pencher sur une décision du Conseil canadien des relations du travail (CCRT) quant à son refus de donner à un plaignant accès aux notes des arbitres.

Le plaignant avait porté plainte contre son syndicat auprès du CCRT—organisme quasi judiciaire—qui statue sur des causes touchant les relations industrielles d'organismes sous juridiction fédérale.

Insatisfait de la décision du Conseil, le plaignant a demandé à voir les notes prises par les arbitres. (Quoique les auditions du Conseil soient publiques, il arrive souvent qu'on n'enregistre pas les séances,

Devant les tribunaux

La vie privée, aussi importante que l'accès à l'information

La Cour d'appel fédérale, dans l'arrêt du ministre des Finances *c. Michael A. Dag* (A-675-93), vient de confirmer que la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels ont un statut égal et que la communication de renseignements en vertu de la première doit respecter les dispositions de la seconde. Le Commissaire à la vie privée du Canada, insatisfait du jugement de première instance qui reléguait la *LP RP* au second rang, est intervenu dans l'appel du ministère des Finances.

M. Dag, consultant du secteur privé, avait demandé que le ministre des Finances lui fournisse les fiches des signatures remplies par les employés faisant des heures supplémentaires à des jours précis entre les 1er et 30 septembre 1990. Il voulait déterminer combien de membres de l'Association des économistes, sociologues et statisticiens (AESS) de la fonction publique faisaient régulièrement des heures supplémentaires. M. Dag entendait calculer le nombre total d'heures de travail et vendre cette information à l'AESS en prévision de la prochaine ronde de négociations collectives. Le ministre lui a remis une copie des fiches demandées, mais a supprimé les noms des employés, les numéros d'identification et les signatures.

M. Dag a déposé une plainte auprès du Commissaire à l'accès à l'information. Celui-ci a donné raison au ministre, estimant qu'il s'agissait de renseignements personnels. Dég, M. Dag en a appelé en première instance de la décision du ministère auprès de la Cour fédérale. Le juge Cullen a conclu que les renseignements demandés n'étaient pas des renseignements personnels mais plutôt de nature professionnelle. Il était d'avis que les organismes gouvernementaux devaient protéger les seuls renseignements dont la caractéristique dominante est d'une nature personnelle. Il a ajouté que "lorsque l'on se demande si des renseignements constituent des "renseignements personnels" qu'il faut divulguer au public ou non, il convient d'accorder le bénéfice du doute à l'interprétation qui favorise la communication des renseignements[...]".

[Traduction]

de la vie privée des habitants de la province, car elle impose des limites aux activités du gouvernement provincial en matière de collecte, d'utilisation et de communication des renseignements personnels qui les concernent. Les citoyens de la Nouvelle-Écosse ont aussi le droit d'accès aux renseignements personnels à leur sujet détenus par les ministères, les organismes municipaux, les conseils scolaires et les universités, et ils peuvent les faire corriger, le cas échéant. Les plaintes sont confiées à un agent d'examen nommé par le gouvernement provincial.

L'Île-du-Prince-Édouard est la seule des provinces et des territoires du Canada à ne pas avoir adopté une forme quelconque de loi sur l'accès à l'information et sur la protection de la vie privée ou des renseignements personnels. Néanmoins, à la suite du discours du Trône prononcé en mars 1994 à la législature provinciale, un comité de députés a étudié la nécessité d'une telle loi. Il en a recommandé l'adoption, et son rapport contient une proposition de libellé qui semble s'inspirer de la loi albertaine. Si le gouvernement provincial de l'Île-du-Prince-Édouard appliquait les recommandations du comité, la boucle serait bouclée dès 1996.

Bien sûr, la vie privée dans le secteur privé n'est protégée qu'au Québec.

... et à l'étranger

L'Union européenne (UE) a adopté sa *Directive sur la protection des données* le 20 février 1995 et celle-ci a été expédiée au Parlement européen pour ratification. La *Directive*, proposée au départ en septembre 1990, fixe les règles de protection de la vie privée des Européennes et Européens et contrôle le traitement et la communication des renseignements personnels qui les concernent. Il est possible que l'article 25 de la *Directive* pose des difficultés aux entreprises canadiennes qui font des affaires en Europe, étant donné qu'elle interdit aux pays membres de l'UE d'échanger des renseignements personnels avec d'autres pays n'ayant pas de lois suffisamment strictes pour protéger ces renseignements sur leur territoire. Or, sauf au Québec, nous n'avons pas au Canada de loi capable de protéger les renseignements personnels du secteur privé, et les codes proposés, dont l'application est volontaire, ne satisfont pas aux critères de la *Directive* européenne.

Mise à jour : Petit à petit, la boucle est bouclée

au Canada...

En juin 1994, l'Alberta a enfin adopté sa loi tant attendue sur l'information et la protection de la vie privée. À partir d'octobre 1995, la *Freedom of Information and Protection of Privacy Act* permettra aux Albertains d'avoir accès aux documents gouvernementaux d'ordre général, ainsi qu'aux renseignements personnels les concernant détenus par le gouvernement, les organismes municipaux, les universités, les conseils scolaires et les organismes responsables des soins de santé. De plus, la loi protégera la vie privée des citoyens en imposant des limites aux activités de collecte, d'utilisation et de communication des renseignements personnels à leur sujet menées par les ministères provinciaux. Le commissaire albertain (qui cumule les fonctions de Commissaire à l'éthique gouvernementale) sera chargé de faire enquête sur les plaintes et de contrôler l'application de la loi, qui lui donne le pouvoir de rendre des ordonnances exécutoires.

En septembre 1994, le gouvernement des Territoires du Nord-Ouest a lui aussi adopté une loi comparable, l'*Access to Information and Protection of Privacy Act*, grâce à laquelle le public aura accès aux documents de ses organismes; en outre, les habitants des Territoires pourront obtenir les renseignements personnels qui les concernent que ces organismes possèdent, et ils pourront demander de les faire rectifier au besoin. La loi s'inspire de celles de l'Alberta, de la Colombie-Britannique, de l'Ontario, du Québec et de la Saskatchewan, quoiqu'avec des exceptions un peu plus générales. Elle entrera en vigueur en décembre 1996. Les limites qu'elle impose à la collecte, à l'utilisation et à la communication des renseignements personnels par les organismes territoriaux mettront le régime de protection de la vie privée des Territoires du Nord-Ouest au diapason de ceux du reste du pays. Les enquêtes sur les plaintes seront confiées à un ombudsman.

La version révisée de la *Freedom of Information and Protection of Privacy Act* de la Nouvelle-Écosse est entrée en vigueur en juillet 1994. C'est la quatrième version de la *Freedom of Information Act* depuis 1977, mais la première à comprendre des dispositions expresses de protection

soumise au Commissariat à des fins de révision. Notre personnel a apporté plusieurs suggestions et les lignes directrices sont maintenant terminées. Elles stipulent:

- Le non-examen des déclarations d'impôt sur le revenu lors des évaluations annuelles de rendement des employés;
- Le maintien de la confidentialité des déclarations d'impôt des contribuables utilisées en preuve lors des procédures de griefs et d'arbitration;

■ L'autorisation obligatoire d'un sous-ministre adjoint pour l'utilisation d'une déclaration d'impôt dans le cadre d'une enquête impliquant le bris de l'une ou l'autre des lois (telle l'utilisation de renseignements internes à des fins personnelles ou encore la modification d'une déclaration d'impôt afin de faire bénéficier ou de nuire à quelqu'un;

■ L'établissement d'un tracé de vérification en conservant au sein de la division de la sécurité les demandes de consultations ainsi que les raisons à l'appui de ces demandes;

■ La protection de la confidentialité des contribuables dont les déclarations d'impôt sont utilisées comme preuve juridique à l'encontre d'employés (en interdisant la publication de ces dossiers, en camouflant l'identité des contribuables ou en procédant à des audiences à huis-clos).

Le sous-ministre a également accepté d'avertir les employés de chaque demande de consultation par un directeur de leurs déclarations d'impôt.

Le Commissariat vérifiera si ces lignes directrices sont effectivement respectées.

Mise à jour : Coopération et mesures de protection des rapports d'impôt

Grâce aux efforts des employés de Revenu Canada, du Syndicat des employés du ministère et du Commissariat, des mesures de protection rigoureuses ont été mises en place quant à l'utilisation des renseignements des contribuables dans le cadre de la surveillance des employés de Revenu Canada.

Un délégué syndical avait fait part par écrit au Commissaire des appréhensions de ses membres quant aux modifications proposées à la *Loi de l'impôt sur le revenu* et à la *Loi sur la taxe d'accise* (rapport annuel de 1992-1993). Leurs préoccupations principales avaient trait aux propositions plutôt générales qui permettaient à Revenu Canada l'utilisation des renseignements des contribuables à des fins de supervision, d'évaluation ou d'imposition de mesures disciplinaires aux employés. Ce faisant, les employés de Revenu Canada auraient été assujettis à une surveillance beaucoup plus sévère que les autres employés fédéraux; en outre, la vie privée des contribuables aurait été affectée par l'utilisation que Revenu Canada aurait faite de leurs dossiers d'impôt à des fins autres que celles pour lesquelles ils avaient été constitués.

L'intégrité du système d'impôt n'a été à aucun moment remise en question; cependant, les modifications avaient été ébauchées de manière si générale qu'elles auraient pu générer des abus. L'intégration de ces utilisations dans la *Loi de l'impôt sur le revenu* annule une disposition de la *Loi sur la protection des renseignements personnels* qui défend l'utilisation des renseignements recueillis dans un but précis (remplir les déclarations d'impôt sur le revenu) pour un autre but (la supervision des employés). Le Commissaire a écrit à Revenu Canada et au Comité des finances de la Chambre des communes et recommandé des mesures de protection plus rigoureuses.

Revenu Canada a proposé d'ébaucher des lignes directrices établissant les critères d'utilisation et créant des contrôles pour les gestionnaires désirant revoir les déclarations d'impôt de contribuables et d'employés dans le cadre d'une enquête. Cette ébauche a aussi été

Les auteurs de ce modèle de loi en résument l'intention ainsi :

L'objet fondamental de cette Loi, c'est qu'aucune personne inconnue de l'intéressé ne devrait posséder ou contrôler des échantillons identifiabiles d'ADN ou d'information génétique sur lui, à moins qu'il n'autorise expressément la collecte de ces échantillons pour fins d'analyse génétique et la création de cette information privée, n'y ait accès et n'en contrôle la diffusion.

Les règles protégeant l'intimité génétique doivent être claires et connues des médecins, des scientifiques, des gens d'affaires, des avocats et du public. La "*Loi sur l'intimité génétique*" a pour raison d'être de codifier ces règles.

Bien qu'elle ait été conçue pour un public américain, la "*Genetic Privacy Act*" contient de nombreux éléments qu'on pourrait reprendre dans une loi canadienne. Fort de ce modèle législatif, le Parlement a encore moins d'excuses de temporiser, plutôt que de contrer sans tarder ce danger croissant pour notre intimité génétique.

■ l'analyse des échantillons doit être utilisée seulement afin de confirmer ou d'infirmer la correspondance entre l'échantillon prélevé sur les lieux du crime et celui provenant du suspect;

■ il faut détruire tous les échantillons d'ADN (et toutes leurs analyses) si le procureur de la Couronne ne porte pas d'accusation, s'il retire son accusation, s'il la suspend, ou encore si l'accusé est acquitté.

Cependant, les recommandations du Commissariat n'ont pas été toutes reprises dans le projet de loi. La plus importante de celles-ci vise à déterminer si c'est l'échantillon ou seulement son analyse qui sera conservé, pour combien de temps, et comment. Le ministre s'est engagé à apporter des modifications plus tard cette année à la question délicate de la conservation des échantillons ou leur analyse. En outre, on devra déterminer les droits des accusés d'accéder aux échantillons prélevés sur les lieux du crime pour permettre une analyse indépendante.

Un autre point en suspens à trait au couplage des analyses d'échantillons obtenus avec un mandat sur les lieux d'un crime à celles d'autres échantillons recueillis ailleurs. Nous avons bien hâte de prendre connaissance des modifications à venir sur les règlements de conservation et les utilisations subséquentes des données.

Intimité génétique

Le projet de loi C104 génère un certain optimisme. Mais nous le sommes moins en ce qui a trait à la protection de l'intimité génétique dans d'autres domaines, notamment ceux de l'emploi, des assurances et de la reproduction humaine. Il est peut-être temps pour les autres ministères fédéraux et en fait pour tous les gouvernements de se pencher sur la législation de ces collectes et l'utilisation des analyses de l'ADN.

La publication plus tôt cette année d'un modèle de «Loi sur l'intimité génétique» ("*Genetic Privacy Act*") par la Faculté de santé publique de l'Université de Boston pourrait bien faire démarrer le processus au Canada.

Le gouvernement fédéral est conscient de la nécessité de réglementer l'ampleur de cette technique. Avec ce rapport qui est en préparation finale, la Chambre de Communes a adopté le projet de loi C104 visant à amender le *Code criminel* et la *Loi sur les jeunes contrevenants* afin d'inclure l'analyse de l'ADN dans les tests criminologiques. Une fois adopté ce projet de loi (actuellement devant un comité du Sénat), établira un cadre de travail pour la collecte et l'utilisation de l'ADN comme preuve lors d'enquêtes criminelles.

Quoique cette loi semble, du moins aux yeux du public, avoir été ébauchée à la hâte, le ministère de la Justice avait rendu public dès septembre 1994 un document de consultation sur l'obtention et la conservation de l'ADN comme élément de preuve criminologique. Dans ce document, le ministère accordait une très grande importance aux implications pour la vie privée des analyses de l'ADN, en se fondant sur notre rapport de 1992 intitulé *Le dépistage génétique et la vie privée* et en faisant siennes, plusieurs des recommandations que le Commissariat à la protection de la vie privée y mettait de l'avant.

En janvier 1995, le Commissariat a réagi au document du ministère de la Justice en reconnaissant l'utilité de l'analyse criminologique de l'ADN, mais non sans réserves. Le projet de loi C104 traite, ou plutôt entend traiter de la plupart de ces inquiétudes dans la dernière ronde de modifications à venir plus tard cette année. Ces modifications auront trait à la conservation et l'utilisation des échantillons (ou leur analyse).

Plusieurs des éléments du projet de loi C104 concernant la collecte et l'utilisation des échantillons d'ADN reflètent la pensée du Commissariat à cet effet. Ainsi,

- un juge doit autoriser la collecte de l'échantillon du suspect;
- les analyses sont limitées à une série de crimes désignés violents qui sont d'ordre sexuel ou/et commis avec violence;
- l'échantillon de l'ADN doit être pertinent à établir le crime, et de l'ADN doit avoir été prélevé sur les lieux du crime afin de pouvoir le comparer avec celui du suspect;

Pourtant, ce genre de surveillance ne semble interdit par aucune loi fédérale, bien que plusieurs provinces reconnaissent des délits civils en matière de vie privée, tandis que le Code civil et la Charte des droits de la personne du Québec protègent les citoyens contre ceux qui voudraient les épier. Les parents qui décideraient de violer ainsi la vie privée de leurs enfants et de trahir leur confiance s'exposeraient à des poursuites au civil. En outre, leurs enfants pourraient leur retourner la balle, en soumettant eux-mêmes au test ceux qui auraient abusé de leur confiance. Voulons-nous que notre société s'engage dans cette voie?

Un test comme celui-là a par ailleurs un intérêt certain pour les employeurs : contrairement à l'analyse d'urine, il n'est pas nécessaire que l'employé soit mis au courant du test ou qu'il y consente, et l'on peut l'administrer sans jamais attirer l'attention des organismes de défense des droits de la personne. L'opposition énergique dont fait preuve le Commissaire quant à l'analyse d'urine n'est rien en comparaison de ce qu'il pense de ces méthodes détournées de dépistage des drogues. Même s'il n'a aucun pouvoir législatif pour interdire ce genre de test, il n'hésitera pas à diriger le chœur de ceux qui réclament des lois pour le prévenir.

Analyses de l'ADN et enquêtes criminelles

On a aussi constaté des progrès sur le front des analyses de l'ADN et plus particulièrement en ce qui a trait aux contrôles juridiques des analyses de l'ADN.

Le procès d'O.J. Simpson aura au moins réussi à sensibiliser tout le public à cette technique naguère nébuleuse. L'analyse criminologique de l'ADN est un instrument d'identification fort utile pour la condamnation ou l'exonération des personnes soupçonnées ou même condamnées pour des crimes violents. Au Canada, l'exemple le plus récent de l'utilisation de ce type d'analyse est le cas de Guy Paul Morin, qui avait été accusé et reconnu coupable du meurtre à caractère sexuel d'une enfant. À la fin de janvier 1995, une analyse perfectionnée de l'ADN a prouvé une fois pour toutes—dix ans après son arrestation—que M. Morin avait été victime d'une erreur judiciaire.

Cependant, la technique est si intrusive qu'il faut soigneusement régler les circonstances dans lesquelles on exigerait d'un suspect qu'il se soumette à un prélèvement d'ADN.

Ramasse-poussière antidrogue

Dans le secteur privé, les nouvelles sont moins prometteuses. À la fin de mars, une entreprise américaine a lancé une trousse maison de dépistage des drogues, la « Drug Alert », à l'intention des parents inquiets et des employeurs soupçonneux.

La trousse contient un morceau de tissu humidifié que l'on passe sur les poignées de porte, les plans de travail et les vêtements pour y ramasser des traces de drogues illégales. Ensuite, on met le morceau de tissu dans une enveloppe et on le renvoie pour analyse au producteur, lequel s'engage à détecter la présence d'une trentaine de drogues illégales.

À supposer que le test soit précis, l'information qu'il génère serait ambiguë, car rien ne confirmerait que la personne visée ait consommé de la drogue : le test détecte simplement des traces de drogue, ce qui n'est certainement pas une preuve de culpabilité puisque l'intéressé peut avoir eu des contacts avec des consommateurs de drogue, ce qui suffirait à laisser un résidu décelable par le test. Tous ceux qui touchent des billets de banque américains (et probablement canadiens) risquent d'y ramasser des traces de cocaïne, vu qu'on les roule souvent en pailles pour inhaler la drogue.

Toutefois, l'aspect le plus inquiétant de la trousse, c'est que son marketing mise sur la crainte bien compréhensible des parents que leurs enfants consomment de la drogue. La rhétorique américaine de la guerre contre la drogue a franchi nos frontières en faisant croire — à tort — aux parents canadiens que la consommation de drogue se répand rapidement chez les étudiants dans notre pays. Il est vrai que certains étudiants consomment des drogues illégales, mais les statistiques les plus récentes du Centre canadien de lutte contre les toxicomanies révèlent que, quoiqu'il y ait des fluctuations, les chiffres sont à la baisse comparativement aux données des années 1970.

La trousse est un moyen pour les parents d'épier leurs enfants et à ce titre, est une invasion cachée de leur vie privée. Dans ce contexte, les conséquences d'une erreur risqueraient d'être fatales pour les relations parents-enfants. Déjà, nous avons craint que l'État, puis le secteur privé ne s'immiscent dans notre vie privée; devons-nous désormais nous

métier de notre propre famille?

argement consommée dans les Forces, au point qu'on pourrait alléguer que c'est celle dont ses membres abusent le plus souvent.

Or, une analyse approfondie de la consommation de drogues et l'alcool des membres des Forces, fondée sur les statistiques que le MDN avait recueillies en 1989 à l'occasion de son sondage sur le mode de vie des Forces, a révélé que les militaires déclarent rarement avoir consommé des drogues illégales, contrairement à leurs collègues civils. En effet, environ 6 p. 100 des membres des Forces avaient consommé de la marijuana au cours de l'année précédente, soit un peu moins que la moyenne de la population. Par contre, ils buvaient plus souvent; 74 p. 100 d'entre eux avaient déclaré avoir consommé de l'alcool au cours de la dernière année, comparativement à 78 p. 100 pour l'ensemble de la population canadienne.

Puisque le sondage du MDN lui-même n'a pas réussi à prouver que les membres des Forces avaient un problème grave de consommation de drogue, le Commissaire a communiqué au début de 1994 avec le Chef d'état-major de la Défense pour s'opposer au programme de tests aléatoires auxquels les militaires étaient couramment soumis.

En février 1995, le Chef d'état-major actuel, le général A.J.G.D. de Chastelain, a avisé le Commissaire qu'il interrompait définitivement les tests aléatoires, l'un des aspects les plus contestables du programme. Toutefois, il s'est réservé le droit de rouvrir la question si les circonstances devaient l'exiger.

C'est un événement important dans les annales du dépistage des drogues au Canada. La décision du général de Chastelain de suspendre les tests aléatoires de dépistage des drogues est une grande victoire pour le bon sens; elle donne l'exemple aux organisations du secteur public et du secteur privé qui envisagent d'avoir recours au dépistage des drogues comme solution miracle à des problèmes qu'ils croient avoir en milieu de travail.

Le MDN va s'en remettre globalement à l'éducation et au counselling, mais il continuera d'administrer des tests de dépistage consécutifs aux accidents, afin de déterminer si la consommation d'alcool ou de drogues illégales y a contribué. D'après ses propres rapports, sur une période de deux ans, la consommation de drogue n'avait rien eu à voir dans les neuf accidents ayant fait l'objet d'une enquête.

Mise à jour : Surveillance du dépistage des drogues

La surveillance des activités de dépistage des drogues de l'administration fédérale se maintient. Les programmes obligatoires de dépistage, tant vantés comme solution miracle de la toxicomanie chez les employés, portent gravement atteinte à la vie privée, car ils forcent ces derniers à fournir des échantillons pour que l'on puisse vérifier leur comportement antérieur.

Le caractère intrusif de ce procédé et l'approche quasi policière qu'il implique sont tels que ses partisans — ils sont nombreux — doivent justifier leurs actes, en démontrant que la toxicomanie cause des problèmes au travail et que le dépistage permet d'atteindre un objectif valable, comme une amélioration de la sécurité, alors que d'autres méthodes moins intrusives n'y arriveraient pas.

Pour certains, cette position peut sembler favorable à la consommation de drogues illégales, mais ce n'est vraiment pas le cas. Il est clair que pour lutter efficacement contre la toxicomanie, il faut éduquer les gens, les appuyer, les traiter et même dans certains cas, éliminer du lieu de travail les conditions susceptibles de causer ou d'exacerber les problèmes des employés. Ce n'est pas en se méfiant constamment d'eux et en les pointant du doigt que l'on trouvera une solution.

Le ministère de la Défense nationale renonce à ses tests aléatoires

L'une des premières constatations de la position du Commissariat a résulté d'un décret de mai 1992 autorisant le ministère de la Défense nationale (MDN) à mener une vaste gamme de programmes de dépistage parmi les membres des Forces canadiennes. On prévoyait des tests aléatoires, aussi bien à caractère dissuasif que consécutifs aux accidents, lorsque l'on avait des soupçons et dans le cadre d'un programme de probation ou de traitement pour les personnes qui avaient consommé de la drogue. Les substances ciblées étaient les drogues illégales et non l'alcool, alors que ce dernier est la drogue la plus

Ce code des plus complets a été conçu par le secteur privé, à l'intention du secteur privé. C'est un début encourageant.

Le Commissariat s'est intéressé au projet de la CSA il y a quatre ans, bien déterminé à appuyer tout ce qui pourrait favoriser nettement les droits des Canadiennes et des Canadiens à la vie privée. À l'époque, un modèle de code d'observation volontaire était de bon ton. Toutefois, il faut que les solutions évoluent en fonction des risques posés par la technologie. Il est évident qu'un code d'autoréglementation dont l'application se ferait sur une base volontaire n'est plus de mise face aux énormes implications sociales du changement technologique, sans parler des inquiétudes croissantes du public. Se fier à un système de protection de la vie privée purement volontaire à l'ère de l'Internet, du Pharnet, des portefeuilles électroniques et des cartes à mémoire, c'est être prêt à avaler n'importe quoi.

Les déclarations d'intention ne suffisent plus. Les Canadiennes et les Canadiens ont besoin de plus et méritent mieux. Seuls seront efficaces des droits à la vie privée garantis par la loi et un organisme de surveillance indépendant. Le combat serait pour le moins inégal si l'on alignait les droits à la vie privée de l'individu contre les possibilités de profits de la commercialisation des bases de données, par exemple. Les codes d'application volontaire ne font pas que priver le public de la protection de la loi : ils risquent de nous inciter à croire aux chimères.

Le Code de la CSA pourrait revêtir toute son importance non pas sous sa forme proposée, en tant que code d'application volontaire à l'intention des entreprises, mais bien par son intégration dans une loi-cadre nationale. Celle-ci en ferait une norme nationale de protection de la vie privée que tous les secteurs devront respecter. Le Conseil consultatif sur l'autoroute de l'information a d'ailleurs reconnu que le Code devrait être la pierre angulaire d'une loi doublée d'un mécanisme de surveillance efficace. Le Commissaire ne peut qu'applaudir à cette conclusion.

Néanmoins, il faut que les règles soient claires, que tout le monde les respecte et qu'elles soient applicables. Un code de protection de la vie privée que les entreprises peuvent décider de ne pas appliquer, ce n'est tout simplement pas assez.

Mise à jour : Le code-type de protection de la vie privée dans le privé

Le projet le plus ambitieux de protection de la vie privée dans le secteur privé vient de l'Association canadienne de normalisation (la CSA), qui s'est efforcée de produire un code-type à l'intention des entreprises canadiennes. Cette initiative de la CSA a réuni un groupe de travail formé de divers représentants du secteur public et du secteur privé en vue d'élaborer une norme de protection de la vie privée à laquelle toutes les parties pourraient souscrire.

Ce groupe de travail comprenait des utilisateurs de données, des organismes représentant les sujets de ces données (employés et consommateurs), l'industrie de la technologie, et les commissaires à la protection de la vie privée du fédéral et de l'Ontario.

La tâche a été dure, mais elle a été couronnée de succès. Le groupe a fait circuler sa première ébauche afin d'obtenir les commentaires du public le 31 décembre 1994 et le verdict a été prononcé. Les principes fondamentaux énoncés dans le Code sont au moins aussi bons, voire meilleurs que ceux qui figurent dans la *Loi sur la protection des renseignements personnels*.

Le premier principe élaboré responsabilise chaque organisme quant aux renseignements personnels sous son contrôle et exige qu'une personne soit responsable de l'adhérence de l'organisme aux autres principes d'information. Au nombre de ceux-ci, nous retrouvons l'identification des objectifs de la collecte de renseignements, ainsi que le besoin de s'assurer que la personne les sache et soit consentante, de recueillir des renseignements de façon juste et conforme à la loi, de limiter la collecte, l'utilisation et la communication des renseignements personnels, de s'assurer de l'exactitude des données recueillies et de les protéger, de rendre ses politiques et ses pratiques de traitement des renseignements personnels facilement accessibles, d'offrir aux personnes l'accès à leurs renseignements personnels et leur donner le droit d'en contester l'exactitude et de s'assurer qu'ils soient complets, et d'offrir aux personnes les moyens de contester l'observation de ces principes par l'organisation.

Le gouvernement fédéral s'est rendu compte du besoin d'une telle infrastructure, et a commencé ses démarches en ce sens, évaluant les besoins des organismes, mettant de l'avant un concept opérationnel, et travaillant de concert avec le secteur privé à l'élaboration d'une norme uniforme.

Mais il faudra encore bien des débats publics avant que le gouvernement ne cède à une quelconque agence les clés du royaume.

Pour résoudre le problème, il faudra confier à un organisme qui aura notre confiance la tâche de créer les paires de clés, de certifier leur validité et d'en gérer la distribution en toute sécurité. Bref, il nous faut un administrateur central capable d'attester de l'identité et de la validité des utilisateurs des clés publiques et privées et d'assurer la sécurité du système. Cet administrateur devra aussi gérer les clés, notamment en produisant un répertoire des clés publiques, pour faire en sorte que les utilisateurs aient accès aux clés publiques les uns les autres, en plus de diffuser des avis publics sur les clés qui ne seraient plus confidentielles ou qui auraient été révoquées.

Il reste encore un problème à résoudre : quel sera le système de livraison et d'adresse auquel on pourra faire confiance, l'équivalent du système postal traditionnel? Comment pourrions-nous obtenir notre paire de clés publique et privée, comment savoir qu'une certaine clé publique correspond bien à une certaine personne, et comment obtenir nos clés publiques respectives?

Le codage protège la confidentialité du courrier électronique et la signature numérique prouve l'origine et l'authenticité du message. Combinés, les deux peuvent assurer une protection électronique de la vie privée.

Bâtir une infrastructure de clés publiques

En plus de la signature, le programme de codage calcule également une représentation mathématique unique du message expédié. C'est ce que l'on nomme "Adressage calculé". Le programme de codage du receveur lit le message, en calcule un second adressage calculé, et le compare à celui qui accompagne la signature de l'expéditeur. Si les deux correspondent, cela signifie que le message n'a pas été modifié depuis son envoi.

Intégrité du message—Adressage calculé (Hash Code)

L'ajout d'un bloc signature distinct codé avec la clé privée de l'expéditeur équivaut à signer et sceller un document. En effet, une seule personne dispose de cette clé privée; son identité est donc vérifiable grâce à la clé publique correspondante et ne peut être niée.

La seconde méthode, celle du codage à clé publique, fait appel à deux clés, une publique (que tous connaissent) pour coder les données, et une privée (connue d'une personne seulement) pour les décoder. Les deux clés forment une paire homogène, mais il est impossible de déduire la clé privée à partir de la clé publique.

Celui qui voudrait recevoir des renseignements confidentiels pourrait diffuser largement sa clé publique, par exemple en la publiant dans un répertoire. Tous ceux qui voudraient lui envoyer des messages pourraient se servir de la clé publique pour les coder, et lui seul pourrait les décoder, étant l'unique détenteur de la clé privée correspondante. Personne d'autre ne pourrait les décoder, pas même celui qui les aurait codés.

Signature numérique identifiant l'expéditeur

Les systèmes de communication électronique doivent aussi être en mesure d'authentifier l'expéditeur et le message. La signature manuscrite est la preuve tangible de l'origine d'une lettre conventionnelle et peut aussi servir à distinguer l'original d'une copie. Il est physiquement impossible d'en faire de même avec un document électronique, lequel ne peut qu'indiquer de qui il provient.

N'importe quel message électronique peut être traité; en outre, l'expéditeur peut simplement se faire passer pour quelqu'un d'autre. Plusieurs policiers se sont récemment fait imputer des dire dans des groupes d'échange et des babillards électroniques. Bref, les communications électroniques ont besoin d'une identification numérique équivalant à une signature.

Le codage par clé publique rend cette «signature» possible, en inversant les rôles des clés publique et privée. Il suffit que l'expéditeur code le message avec la clé publique du destinataire, en lui ajoutant sa signature, codée avec sa clé privée.

Le destinataire peut décoder le message de façon normale, avec sa propre clé privée, tout en vérifiant l'identité de l'expéditeur en décodant la signature au moyen de la clé publique de ce dernier.

ou par un système auquel nous pouvons nous fier pour l'acheminer en toute confidentialité. Ni l'expéditeur, ni le destinataire n'ont le moindre contrôle (ni connaissance) de ceux qui peuvent lire leur courrier électronique en transit. Envoyer un message en clair avec un ordinateur, c'est donner à tous ceux qui ont accès au système la possibilité de le lire, de l'enregistrer, de le contrôler, de le trafiquer ou de le détruire avant qu'il n'arrive à destination.

Cela dit, on peut coder le courrier électronique pour le protéger, en confirmant la source et l'intégrité des messages et en les authentifiant avec des signatures numériques.

Codage

Le codage permet de rendre un message en clair intelligible sauf pour son destinataire, qui a seul la clé pour le déchiffrer. On procède en codant le message à l'aide de procédés mathématiques appelés algorithmes, pour transformer le texte en clair en une version codée et vice versa. Les algorithmes sont des systèmes servant à cacher le sens d'un texte, ils sont en quelque sorte l'équivalent électronique des serrures.

Ces "serrures électroniques" ont donc besoin de clés. Ces clés peuvent être des chiffres, des caractères ou des formules (sous forme de bits) dont se sert l'algorithme de codage pour «verrouiller» ou «dévrouiller» un message transformé. La clé de codage va de pair avec l'algorithme qu'elle chiffre ou déchiffre.

Une ou deux clés

De nos jours, il y a deux méthodes courantes de codage, la secrète, qui fait appel à une seule clé partagée, et la publique qui fait appel à deux clés différentes.

Avec la première méthode, à clé unique partagée, l'expéditeur et le destinataire doivent avoir la même clé secrète pour coder et décoder le message. L'inconvénient, c'est précisément qu'ils doivent avoir la même clé. Quand il y a beaucoup de correspondants, l'expéditeur doit partager une clé différente avec chacun des destinataires, en gardant chacune de ces clés secrète.

Néanmoins, le Conseil reconnaît qu'il n'existe aucune mesure ni technologie de sécurité capable d'assurer une protection absolue de l'information. Il recommande un niveau de sécurité de base avec lequel on peut raisonnablement s'attendre à ce que les communications privées et les renseignements personnels soient protégés. Au-delà de ce niveau, le marché aurait l'entière discrétion de concevoir et de vendre une protection renforcée des données de nature plus délicate.

Concilier les droits à la vie privée, les droits civiques et les droits de la personne avec la réalité de l'application des lois et les intérêts de la sécurité nationale sur l'information est impossible sans des études approfondies et des consultations du public. Une des méthodes de protection des communications et des données véhiculées sur l'information consiste à créer une infrastructure de clés publiques.

Pour bien situer le débat, il faut d'abord définir certains concepts.

Aperçu de la sécurité des communications : de la boîte aux lettres au courrier électronique et à l'infrastructure de clés publiques

La sécurité du courrier est depuis longtemps un élément critique de la confiance que nous accordons au service postal. Nous nous attendons à ce que notre courrier soit livré aux destinataires d'une façon qui protège sa confidentialité. Nous le mettons dans des enveloppes cachetées que nous confions à un service postal qui recueille, achemine et livre le courrier.

L'un des éléments fondamentaux du système, c'est que nous savons qu'il est confidentiel et protégé par la loi. Même si une foule de camionneurs, de trieurs et de facteurs touchent à nos lettres, ils ne peuvent pas les lire, parce qu'elles sont cachetées. Nous avons confiance : le système va les livrer au destinataire intactes, sans qu'elles aient été lues ou trafiquées.

Le courrier électronique est simplement une communication transmise par des systèmes d'ordinateurs interreliés plutôt que par la poste. Sa confidentialité n'est pas protégée par des enveloppes cachetées

vie privée. Il a donc conclu que le gouvernement fédéral doit assumer le leadership pour la protection des renseignements personnels.

Même si son rapport final n'est pas attendu avant l'automne,

le Conseil a déjà reconnu publiquement la nécessité d'une norme nationale, applicable à l'ensemble des secteurs public et privé, afin d'assurer la protection de la vie privée des Canadiennes et des Canadiens dans l'univers électronique. À cette fin, il a recommandé

■ l'établissement de règles du jeu égales pour tous grâce à une loi-cadre nationale de protection de la vie privée, créant une norme minimale d'information équitable correspondant au projet de "Code-type pour la protection des renseignements personnels de l'Association canadienne de normalisation";

■ la formation d'un groupe de travail fédéro-provincio-territorial chargé d'appliquer ces principes dans tout le Canada;

■ la mise à jour et l'harmonisation des politiques, dispositions législatives et autres lignes directrices du gouvernement fédéral en matière de protection de la vie privée;

■ la création d'un groupe de travail chargé de coordonner le développement et l'application de technologies de prestation de services et de fourniture de renseignements

gouvernementaux qui renforcent la vie privée de la population.

Fait particulièrement encourageant, le Conseil reconnaît que

les normes d'application volontaire sont utiles pour amener les entreprises à protéger la vie privée, mais que le gouvernement doit s'efforcer de mettre en place des mécanismes efficaces de surveillance et d'application afin de protéger la clientèle des entreprises qui refusent ce «volontariat».

Assurer la sécurité

La sécurité est une question d'importance critique dans les réseaux interactifs, car il s'agit de protéger aussi bien les données emmagasinées que les communications personnelles et d'affaires.

Mise à jour : La vie privée, la sécurité et l'autoroute de l'information

L'an dernier, peu de sujets ont fait couler plus d'encre ou fait plus de bruit que l'autoroute de l'information. Pourtant, dans tout ce battage, on a à peine entendu l'appel du Conseil consultatif sur l'autoroute de l'information, qui a réclamé "une intervention du gouvernement fédéral pour assurer la protection de la vie privée sur l'information".

Le Conseil est un groupe mixte de représentants de l'entreprise privée, des consommateurs et des universités, créé par le gouvernement fédéral afin d'élaborer une stratégie sur l'autoroute canadienne de l'information. Il s'est penché notamment sur la protection de la vie privée ainsi que sur la question connexe de la protection des systèmes interactifs et des données qui y sont véhiculées.

Il va sans dire que les notions de vie privée et de sécurité ne sont pas synonymes. Les distinctions sont de taille, car un réseau de données sûr peut être protégé contre les intrusions d'utilisateurs importuns, sans toutefois offrir aux sujets des données la moindre protection contre une collecte abusive et une mauvaise utilisation des renseignements personnels qui les concernent, ni contre leur communication injustifiée par les contrôleurs et les utilisateurs autorisés.

Protection de la vie privée

Le document de travail du Conseil, intitulé *La protection de la vie privée et l'autoroute canadienne de l'information*, est un exposé des dangers pour la vie privée dans lequel les Canadiennes et les Canadiens se font demander leur avis sur la façon de concilier la liberté de l'information et la menace pour la vie privée que constitue l'information.

Les réponses du public, y compris celle du Commissariat, ont persuadé le Conseil que la population s'inquiète de la menace que l'autoroute de l'information fait planer sur ses renseignements personnels, médicaux et financiers, et qu'elle souhaite une protection efficace de sa

En résumé, le gouvernement fédéral devrait renforcer la protection de la vie privée des Canadiennes et des Canadiens en

■ étendant la portée de la *Loi sur la protection des renseignements personnels* aux domaines d'activités du secteur privé qui relèvent de sa compétence et en

■ chargeant un groupe de travail fédéral-provincial d'harmoniser la législation sur la protection de la vie privée dans le secteur privé de compétence provinciale.

Pour revenir à Jules César, ne ratons pas la marée montante.

Maintenant, nous sommes à flot au large;
Profitions des courants, tandis qu'ils sont
propices,

Ou nous perdrons nos chances. [Traduction]

—Jules César, acte IV, scène III

On ne peut plus prendre notre temps

complètement et uniformément. Or, il faudra vraisemblablement beaucoup plus de temps que ne le permet l'urgence de la situation pour arriver à un résultat pareil. Le progrès technologique poursuit sa course effrénée, et si personne n'agit avant que tous se donnent la main pour le faire, nous aurons perdu une grande partie de ce qui peut encore être sauvé.

Puisque le problème est d'envergure nationale, c'est naturellement au gouvernement national qu'il incombe de faire preuve de leadership. Heureusement, certains des principaux secteurs d'activité commerciale sont de compétence fédérale, tels ceux des télécommunications, des transports et des banques, trois des plus importants secteurs qui recueillent et utilisent des renseignements personnels. Le gouvernement fédéral, sans outrepasser sa propre compétence, est donc en mesure de saisir l'initiative et d'assujettir ces secteurs d'activité privée à la *Loi sur la protection des renseignements personnels*, comme il l'a déjà fait avec ses lois sur les droits de la personne, les langues officielles et les relations du travail.

Le gouvernement pourrait en outre ajouter à la *Loi sur la protection des renseignements personnels* des dispositions conçues expressément pour le secteur privé, comme le code-type de protection de la vie privée élaboré par l'Association canadienne de normalisation (la CSA).

Cette deuxième possibilité présente d'intéressants avantages, car elle permettrait d'enchâsser dans une loi un ensemble de règles formulées par un comité largement représentatif de l'entreprise privée canadienne. La principale amélioration serait que l'observation de la norme de la CSA deviendrait une obligation légale appuyée par un système de surveillance indépendant. En outre, cette solution est susceptible d'être acceptée par les provinces, puisque les entreprises représentées au comité qui a produit le code-type de la CSA oeuvrent dans les deux sphères de compétence, la fédérale et la provinciale. Par ailleurs, plusieurs commissaires provinciaux à la protection de la vie privée ont souscrit au code en disant que ce serait un excellent point de départ pour une loi de ce genre. Nous avons donc là un ensemble de règles de protection de la vie privée déjà largement accepté aux paliers tant fédéral que provincial, auquel il ne manque que le cadre d'une loi.

Baliser le terrain

Le danger d'avoir recours à divers organismes sectoriels de protection de la vie privée, c'est que la culture de ces organismes tend à refléter énormément celle des secteurs qu'ils réglementent ... et à leur être sympathique. Ceux pour qui c'est d'abord et avant tout la protection de la vie privée qui doit primer doivent avoir une véritable indépendance d'esprit. Nous n'avons pas de polices distinctes pour chaque type de crime, mais bien une police polyvalente qui sert toute la collectivité et que nous entendons voir appliquer également une norme commune dans toute la collectivité.

À mon avis, c'est simple : si le monde change et que le changement menace des droits établis et reconnus, nous devons changer les lois qu'il faut pour renforcer et pour défendre ces droits.

Les conclusions sont incontournables :

- la protection de la vie privée ne peut être laissée au gré du marché; elle a besoin d'être renforcée par des normes légiférées, et elle mérite de l'être;
- la loi doit s'appliquer au secteur public et au secteur privé;
- il faut prendre des mesures aux paliers fédéral et provincial pour harmoniser au maximum les lois et leur application;
- les normes légiférées doivent être étayées par un mécanisme indépendant de surveillance et d'application, sans lequel elles ne seraient que des déclarations d'intention dénuées d'efficacité;

■ il faut que l'impact (social) de la technologie de l'information soit évalué de façon systématique par un organisme indépendant spécialisé, du genre de l'*Office of Technology Assessment* des États-Unis.

Le gouvernement fédéral et les gouvernements provinciaux ont des secteurs de compétence importants dans le monde de l'information. Le mieux serait qu'ils adoptent à peu près simultanément des lois complémentaires, étayées par des mécanismes de surveillance analogues grâce auxquels tout l'univers canadien de l'information serait protégé

Responsabiliser le système

Certains — mal renseignés — diront que cela mènerait tout droit à la création d'énormes bureaucraties, voire d'armées de foudrilleurs gouvernementaux, mais les événements récents leur donnent tort. Il y a moins de deux ans, le gouvernement du Québec a modifié sa législation sur la protection de la vie privée afin d'en étendre la portée à toutes les entreprises privées de la province. Or, le commissaire québécois à la protection de la vie privée a déclaré que la transition s'est faite sans heurts : les entreprises continuent à faire des affaires, le ciel ne s'est pas écroulé, et personne ne s'est plaint d'intrusions excessives ou injustifiées de « foudrilleurs gouvernementaux ». Et quant à l'explosion bureaucratique, même si le commissaire a reçu environ 300 plaintes contre le secteur privé, il n'a ajouté qu'une demi-douzaine de personnes à son effectif.

À cet égard, il vaut la peine de préciser que, en 12 ans d'existence, le Commissariat que je dirige a enquêté sur plus de 10 000 plaintes mettant en cause plus de 10 ministères, organismes et tribunaux fédéraux, et que son effectif n'a jamais dépassé environ 35 personnes. Et le Commissariat a procédé à des vérifications des pratiques de gestion de l'information d'environ le tiers des services gouvernementaux fédéraux, outre ses nombreuses activités de recherche, d'élaboration de politiques et d'affaires publiques. On peut bien parler d'enflure bureaucratique

Cependant, certains tendent de plus en plus à souscrire à l'idée que chaque secteur du monde des affaires devrait avoir son propre défenseur de la vie privée. Par exemple, le Conseil de la radio-télévision et des télécommunications canadiennes serait responsable du secteur des communications, l'Office national des transports de celui des transports, le Bureau du surintendant des institutions financières des banques, et ainsi de suite. À moins que les gens ne soient disposés à renoncer à tous leurs principes sur le refus d'une enflure bureaucratique et sur l'importance de l'uniformité des règles du jeu et des normes, ces arguments devraient être rejetés du revers de la main, comme ils le méritent, car aucun des pays du monde où les entreprises privées sont assujetties à une loi sur la protection de la vie privée (la plupart des pays d'Europe occidentale, la Grande-Bretagne, la Nouvelle-Zélande et l'Australie) ne s'est aventuré dans cette voie semée d'embûches.

l'existence du problème, mais continue largement à résister à l'idée qu'il doit faire plus qu'observer «volontairement» des codes «autoréglementés» de protection de la vie privée. Autrement dit, il reconnaît l'existence d'un problème de circulation, mais refuse d'accepter l'intervention de la police.

Observation volontaire des codes de protection de la vie privée

J'en suis venu—bien malgré moi—to conclure que, dans ce contexte, les codes «volontaires» ne suffisent pas, et ce, pour plusieurs raisons. Premièrement, la collecte de renseignements personnels, en grande partie à notre insu ou sans notre consentement, est désormais une importante activité commerciale qui prend constamment plus d'ampleur. Les individus que nous sommes ont le droit d'exercer un certain contrôle sur ce trafic, mais tout ce qui s'est dit là-dessus ces dernières années n'a eu à peu près aucun effet.

Deuxièmement, le progrès technologique accélère le processus, et le problème s'aggravera jusqu'à ce que soient imposées des normes applicables.

Troisièmement, les protections dont nous bénéficions actuellement risquent d'être sapées par l'interconnectivité imminente des bases de données du secteur public (assujetties à la législation sur la vie privée) avec les bases de données et les systèmes de transmission du secteur privé (qui échappent à toute législation de ce genre).

Quatrièmement, les Canadiennes et les Canadiens ont le droit d'être protégés par des normes uniformes de respect de leurs droits à la vie privée, sans égard à leur lieu de résidence ou à la nature de leurs activités; cette protection sera impossible si le secteur privé est laissé libre d'en décider à son gré.

Cinquièmement, le public n'accordera jamais sa confiance à un système si des règles justes ne sont pas également et équitablement appliquées à tous les éléments de la société, c'est-à-dire aussi bien au secteur privé qu'au secteur public, et si ces règles ne sont pas renforcées par un mécanisme indépendant de surveillance et de règlement des plaintes, autrement dit la police dont j'ai parlé plus haut.

Bien entendu, cette situation est moins attribuable à des efforts individuels qu'à l'accumulation de preuves patentes pour à peu près tout le monde qu'il ne s'agit pas là d'un problème philosophique abstrait, mais bien d'un danger quotidien. Les conditions préalables à une action efficace sont désormais réunies, quelle qu'en soit la raison. Il ne faut toutefois pas confondre la reconnaissance du problème avec sa solution. On parle beaucoup, mais sans grand résultat. Néanmoins, en quelques années, nous avons accompli des progrès réels.

Un fait saute aux yeux : tout se jouera d'ici un an ou deux, et nous saurons alors si notre société tient suffisamment à l'autonomie personnelle et à l'individualité de chacun pour le défendre contre les pressions incessantes des bilans financiers, ou si nous accepterons de n'être que des numéros informatisés.

L'atmosphère est à l'optimisme, quoiqu'avec une certaine nervosité, parce que des voix influentes appuient énergiquement une protection accrue de la vie privée à l'ère de la technologie de l'information. C'est le cas notamment du travail accompli en comité par le Conseil consultatif sur l'autoroute de l'information que le gouvernement a créé (et dont nous reparlerons plus loin). La nervosité s'explique parce que les intérêts privés sont capables de résister au changement et que la conjoncture actuelle n'est pas favorable à l'intervention gouvernementale dans le monde des affaires. Pourtant, même une conjoncture pareille ne saurait justifier qu'on ne protège pas les valeurs qui nous définissent. Les années de vaches grasses et de vaches maigres se succèdent, mais le respect des droits de la personne doit rester le fondement même de la société, dans la prospérité comme dans la disette.

L'enjeu est clair, car si nous voulons continuer d'avoir une vie privée à l'ère de l'information, nous devons conserver un certain contrôle sur ce que l'on sait de nous. Or, ce contrôle est à toutes fins utiles disparu, sauf dans les domaines limités où il existe des lois de protection de la vie privée, particulièrement dans le secteur public. La seule façon de le rétablir, c'est d'avoir de meilleurs moyens de défense juridiques. Ces deux prémisses font maintenant la quasi-unanimité. Le secteur privé canadien, généralement libre de toutes règles législatives sur la vie privée (sauf au Québec), est désormais conscient de la marée montante de l'inquiétude du public. De nombreuses entreprises ont même tenté de l'endiguer en se dotant de leurs propres codes de protection de la vie privée, et c'est précisément le hic. Le secteur privé reconnaît

Nouveaux mots

Or, l'information n'est pas simplement une substance ou une entité; elle n'est pas seulement faite de données; elle n'est pas plus un produit ou une denrée. Qu'elle soit communiquée par la voix ou véhiculée par un enregistrement, un imprimé, une image, un code numérisé, un langage gestuel ou une vision, l'information est l'expression de tout ce que nous savons, voire de tout ce que nous sommes. La substance même de la vie de chacun est exprimée sous forme d'information ou, si l'on préfère, de renseignements personnels, toutes les choses qui distinguent un être humain d'un autre et qui attestent de l'unicité de chaque individu.

En fait, l'expression «vie privée» ne suffit pas à décrire toute l'ampleur de la notion. Dans le contexte de la technologie, certains spécialistes parlent plutôt de «droit à l'autodétermination de l'information» ou de droit de «contrôler ce que les autres savent de soi». Pour bonnes qu'elles soient, ces descriptions n'en sont pas moins des reflets d'une réalité plus profonde encore, la mesure dans laquelle nous nous respectons les uns les autres en tant qu'êtres humains à l'ère nouvelle de l'information.

Nous avons tenté dans les rapports annuels antérieurs de sensibiliser le Parlement et le public au danger mortel que pose l'application universelle ou irréfutable de la technologie de l'information pour le maintien d'un niveau raisonnable de protection de la vie privée. Il faut bien reconnaître que la situation a nettement changé à cet égard, car un sondage après l'autre révèle une inquiétude croissante du public : de 80 à 90 p. 100 des répondants disent craindre qu'on porte atteinte à leur vie privée et soupçonnent—à juste titre—qu'il se passe bien des choses qu'on leur explique mal, et que le pire pourrait bien être à venir.

En outre, les sondages montrent fréquemment que le public a non seulement des craintes, mais aussi de grandes attentes d'intervention gouvernementale. En effet, il sait que le monde se transforme rapidement; il a peur de se retrouver désarmé dans un environnement plus menaçant pour son autonomie personnelle que tout ce qu'il a connu jusqu'à présent. Bref, alors qu'il était naguère largement indifférent à la protection de la vie privée, il lui accorde désormais une priorité—relative sinon dominante—dans la liste des questions qui méritent son attention.

**Il y a une marée dans les affaires humaines.
Quand on saisit le flux, il mène à la fortune;
Quand on le laisse passer, tout le voyage de la vie
Échoue dans les bas-fonds et les misères.** [Traduction]

— Jules César, acte IV, scène III

Qu'en termes élégants ces choses-là sont dites,
M. Shakespeare! Dans le parler d'aujourd'hui, nous dirions probablement
«Allons-y», voire quelque chose de plus direct encore, mais le sentiment
serait le même, car le moment est venu de passer à l'action.

Les événements se sont vite succédés cette année. Nous voilà
rendus au point critique où s'imposent des décisions qui vont nous mener
soit à la fortune, soit dans les bas-fonds et les misères.

Comme ces décisions incombent globalement à nos
gouvernements, je les implore de saisir l'occasion avec courage et
prévoyance, et de résister aux intérêts spéciaux qui feront inévitablement
pression pour leur inspirer des demi-mesures irrésolues. Et timidité n'est
pas vertu, quand il faut défendre les droits de la personne.

Cela dit, prenons un peu de recul pour étudier le contexte dans
lequel nous vivons. La plupart des gens sont désormais conscients de
l'immense portée du changement technologique dans notre société. La
technologie de l'information brille de tous les feux de la connaissance
dans le commerce, le monde universitaire, l'univers des sciences, de la
médecine et du gouvernement, bref, dans tous les aspects de la vie
humaine. Prenons garde que ces feux ne nous aveuglent et nous fassent
oublier notre devoir d'en profiter sans renoncer aux valeurs plus
anciennes, fondamentales pour la protection des droits de la personne, qui
sont le fondement de notre société civilisée.

Au fil des siècles d'évolution de la pensée occidentale, le droit
de chacun de défendre son caractère unique en exerçant un certain
contrôle sur la capacité d'intrusion ou d'imposition d'autrui a toujours été
reconnu, mais la révolution technologique le bat en brèche.

Table des matières

Il y a une marée...	1
Mise à jour : La vie privée, la sécurité et l'autoroute de l'information	9
Aperçu de la sécurité des communications : de la boîte aux lettres au courrier électronique et à l'infrastructure de clés publiques	11
Mise à jour : Le code-type de protection de la vie privée dans le privé	16
Mise à jour : Surveillance du dépistage des drogues	18
Analyses de l'ADN et enquêtes criminelles	21
Intimité génétique	23
Mise à jour : Coopération et mesures de protection des rapports d'impôt	25
Mise à jour : Petit à petit, la boucle est	27
Devant les tribunaux	29
La vie privée, aussi importante que l'accès à l'information	29
On refuse accès à des notes—cas devant les tribunaux	30
Consulter le Commissaire—Pensions des députés fédéraux	31
Enquêtes de plaintes	34
Les cas	37
Demandes de renseignements	57
Vérification de l'observation	65
Aliénation des biens excédentaires de l'État	67
Partage de renseignements personnels—accords et ententes	70
Aviser le Commissaire	76
Vérifications et suivi	79
Consommation et Corporations, Immigration, Administrations de pilotage du Pacifique et de l'Atlantique, Conseil des arts du Canada	79
Suivi	86
Bureau du Directeur général des élections	87
Gestion intégrée	89
Organigramme	91

Faits saillants

- Le gouvernement fédéral doit agir dès maintenant afin de protéger la vie privée des Canadiennes et Canadiens dans le secteur privé. Il doit commencer par les secteurs qui relèvent de sa compétence, soient les banques, les télécommunications et les transports inter provinciaux (page 7)
- Le recensement ne s'effectuera plus de la même façon qu'avant, et protégera mieux la vie privée des citoyens—mais il reste une question sans réponse (page 37)
- Les Forces armées cessent leurs tests aléatoires de dépistage de drogues (page 18)
- Une protection électronique de la vie privée - une infrastructure de clés publiques (page 9)
- Les dossiers des contribuables et des employés seront protégés lors des enquêtes internes de Revenu Canada (page 25)
- Les dossiers de faillite ne contiendront plus de renseignements superflus (page 79)
- L'aliénation de biens fédéraux excédentaires (ordinateurs, disquettes et classeurs) se fera de façon plus rigoureuse (page 67)
- 1 307 enquêtes de plaintes, près de 10 000 demandes de renseignements et un record: 1 783 nouvelles plaintes (page 34)

Notre mission

Voici en quoi consiste la mission du Commissaire à la protection de la vie privée :

■ être un protecteur efficace des droits des citoyens qui mène, en temps opportun, des enquêtes approfondies afin que la population puisse jouir des droits que lui accorde la Loi sur la protection des renseignements personnels;

■ protéger efficacement, au nom du Parlement, la vie privée des citoyens et évaluer de façon professionnelle dans quelle mesure le gouvernement respecte les dispositions de la Loi sur la protection des renseignements personnels;

■ conseiller le Parlement sur les questions liées à la protection de la vie privée, et lui fournir, grâce aux activités de recherche et aux communications, les faits qui lui permettent de rendre des jugements avisés;

■ être le principal centre national de ressources pour la recherche, l'éducation et l'information en matière de protection de la vie privée.

Notre mandat

Le Commissaire à la protection de la vie privée est un ombudsman spécialisé nommé par le Parlement et tenu de lui rendre compte qui surveille la façon dont le gouvernement fédéral recueille, utilise et communique les renseignements personnels de ses clients et de ses employés, et répond aux demandes des personnes souhaitant consulter leurs dossiers.

La Loi sur la protection des renseignements personnels donne au Commissaire de vastes pouvoirs pour enquêter sur les plaintes dont il est saisi, de lancer sa propre plainte et de vérifier si les quelque 110 organismes gouvernementaux assujettis à la Loi en respectent les dispositions. Il effectue aussi des activités de recherche de son propre chef ou à la demande du ministre de la Justice.

Gerard J. C. van Berkel

Gerry van Berkel est décédé six mois à peine après avoir pris sa retraite en tant que conseiller juridique auprès du Commissaire à la protection de la vie privée, poste qu'il a occupé dès la mise sur pied du Commissariat en 1983.

Être humain extraordinaire et avocat exceptionnel, les mots du poète Marvell le décrivent bien [traduction] : "Ses gestes et pensées étaient hors du commun, celui qui a vécu parmi tout un chacun". Pour lui, la loi se voulait améliorer la condition humaine plutôt que la régimenter. On l'a d'ailleurs souvent entendu dire que "la loi ne devait pas empêcher de venir en aide aux gens" et cette attitude, alliée à son grand bon sens et à sa compassion, a fait de lui le conseiller idéal pour un ombudsman.

Avocat au service du gouvernement pendant trois décades, Gerry van Berkel a oeuvré pour le ministère du Travail et également la Commission des droits de la personne. Partout sur son passage, il a attiré amis et admirateurs. Le personnel du Commissariat a bien profité de sa maturité et sa sagesse, de son esprit et sa patience; à preuve, il a toujours tolérer avec humour les "avis juridiques" que certains d'entre nous improvisaient sans fondement.

Mais il était aussi connu comme un raconteur hors pair, un cuisinier extraordinaire, un pianiste émérite de musique pop, un ébéniste doué et surtout un homme dévoué à sa famille et un ami loyal. Bref, l'exemple parfait du travail d'un Créateur en qui il avait une confiance éternelle.

Nous lui dédions ce rapport avec amour et respect.



Commissaire
à la protection de
la vie privée du Canada

Privacy
Commissioner
of Canada

L'honorable Gilbert Parent
Président
Chambre des communes
Ottawa

juillet 1995

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Le rapport couvre la période allant du 1^{er} avril 1994 au 31 mars
1995.

Vous agréer, Monsieur, l'expression de mes sentiments
respectueux.

Le Commissaire à la protection de la vie privée

Bruce Phillips

Bruce Phillips



Commissaire
à la protection de
la vie privée du Canada
Privacy
Commissioner
of Canada

L'honorable Gildas L. Molgat
Président
Sénat
Ottawa

juillet 1995

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Le rapport couvre la période allant du 1^{er} avril 1994 au 31 mars
1995.

Vous en trouverez l'expression de mes sentiments
respectueux.

Le Commissaire à la protection de la vie privée

Bruce Phillips
Bruce Phillips

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 994-2410, 1-800-267-0441
Télec. (613) 995-1501
ATS (613) 992-9190

© Groupe Communication Canada
N° de cat. IP 30-1/1995
ISBN 0-662-61956-0

Cette publication est offerte sur cassette et sur disquette informatique. Nous
sommes accessibles sur le réseau Internet à :

<http://info.ic.gc.ca/opengov/opc/privacy.html>

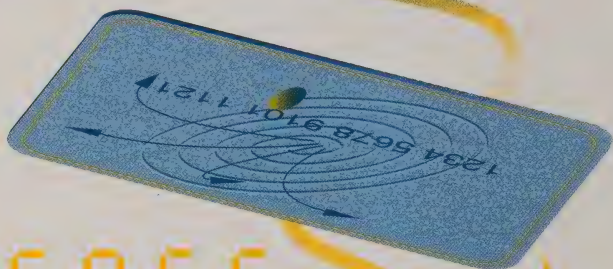
**Rapport annuel du
Commissaire à la protection
de la vie privée
1994-1995**





1994 - 1995

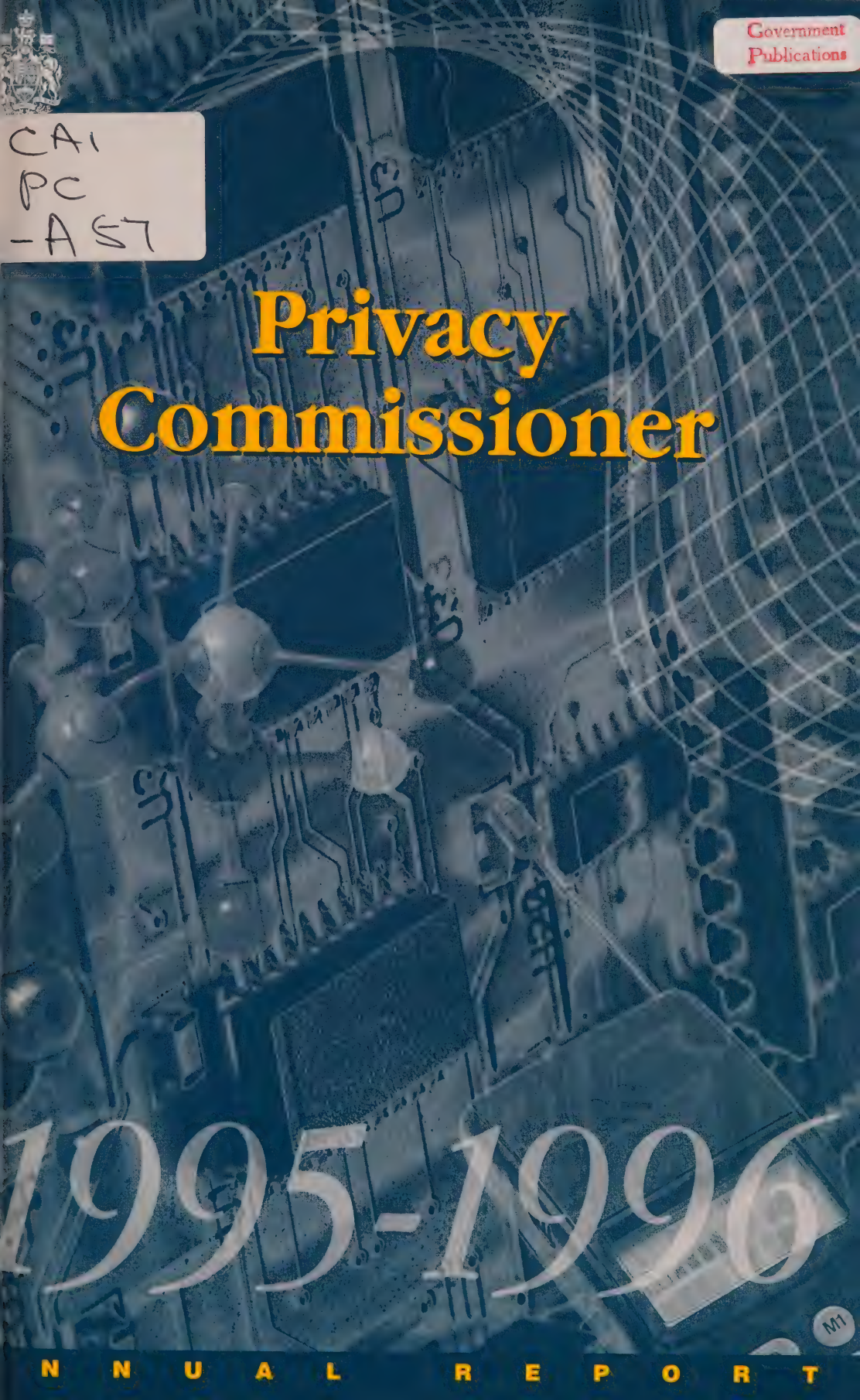
rapport annuel



330985020



Commission de la protection
de la vie privée



CAI
PC
-A57

Privacy Commissioner

1995-1996

CAI
P-
-A57

Annual Report Privacy Commissioner 1995-96



The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-2410, 1-800-267-0441
Fax (613) 947-6850
TDD (613) 992-9190

© Canada Communications Group
Cat. No. IP 30-1/1996
ISBN 0-662-62582-X

This publication is available on audio cassette, computer diskette and on the Office's Internet home page at <http://infoweb.magi.com/~privcan/>



Privacy
Commissioner
of Canada

Commissaire
à la protection de
la vie privée du Canada

The Honourable Gildas L. Molgat
The Speaker
The Senate
Ottawa

July 1996

Dear Mr. Molgat:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1995 to March 31, 1996.

Yours sincerely,

Bruce Phillips
Privacy Commissioner



Privacy
Commissioner
of Canada

Commissaire
à la protection de
la vie privée du Canada

The Honourable Gilbert Parent
The Speaker
The House of Commons
Ottawa

July 1996

Dear Mr. Parent:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1995 to March 31, 1996.

Yours sincerely,

A handwritten signature in dark ink, reading "Bruce Phillips". The signature is written in a cursive style with a large initial "B".

Bruce Phillips
Privacy Commissioner

A Day in the Life...or how to help build your Super File

Nothing to hide? It's just as well...from the time we get up in the morning until we climb into bed at night we leave a trail of data behind us for others to collect, merge, analyse, massage and even sell—often without our knowledge or consent. And there is no law against it (except in Quebec).

- 8:30 **Exit apartment parking lot** (Cameras, and possibly a card, record departure)
- 8:35 **Pull onto toll highway** (Device records your entry and exit points to send bill at the end of the month)
- 8:42 **Caught in traffic jam, call work to delay meeting** (Cellular phone calls can be easily intercepted; new personal telephones will signal your whereabouts to satellites to deliver calls)
- 9:17 **Enter office parking lot** (Card records entry and time, cameras monitor garage)
- 9:20 **Enter main office/plant door** ("Swipe" cards record comings and goings; active badges allow others to locate you anywhere in the building)
- 9:25 **Log on to computer** (System records time in)
- 9:29 **Send personal E-mail to friend, business message to colleague** (Both can be read by the employer; simple deletion does not erase them from the computer's hard drive)
- 10:45 **Call your mother** (Supervisors may monitor phone calls)
- 11:00 **Make a delivery using company vehicle** (Many company vehicles have geo-positioning devices to plot vehicle location; some have "black boxes" to record driving habits)
- 12:05 **Stop at bank machine** (System records details of transactions, cameras overhead or in machine record your behaviour)
- 12:10 **Buy birthday gift for friend** (Credit card records details of purchase, retailer's loyalty card profiles purchase for points and directed discounts; banks may use spending patterns to help assemble complete customer profile)
- 12:35 **Doctor's appointment** (Health cards will soon contain small computer chips to record your complete medical history on the card, blood samples contain DNA which could be tested for wide variety of conditions, doctor's diagnosis may need to be disclosed to insurance company if you buy life or disability insurance and details sent to centralized registry in U.S run by insurance companies)

- 1:15 **Pick up prescription** (Some provinces have on-line drug networks which share your drug history with pharmacies across the province and may be disclosed to police tracking drug abuse)
- 1:30 **Return to work** (Card records your return)
- 2:45 **Provide urine sample for employer's new drug testing program** (Reveals use of targetted drugs but not impairment; sample may also reveal use of legal drugs such as birth control pills, insulin and anti-depressants)
- 3:30 **Meeting in secure area** (Pass through security which scans retina to confirm identity)
- 5:30 **Complete first draft of report** (Computer records content, can also store keyboard speed, error rate, length of pauses and absences)
- 6:15 **Leave office** (Exit recorded by computer, entry system and parking lot)
- 6:30 **Buy groceries** (Debit card purchase recorded, loyalty card tracks selections for marketing and targeted discounts)
- 6:45 **Pick up video** (Computer records viewing preferences, Social Insurance Number; store may sell your viewing preferences—say, Erotica—to other companies)
- 7:20 **Listen to phone messages** (Your phone has recorded callers' phone numbers, displays your number when you call others—unless you enter code to block the display)
- 8:20 **Order clothing from catalogue** (Company records personal details and credit card number and may sell the information to database—list—marketers)
- 8:30 **Subscribe to new magazine** (Many magazines routinely sell their subscribers' list to mass mailers)
- 8:35 **Survey company calls** (Company gathers political views, social attitudes and personal views. Some surveys are actually marketing calls to collect personal data for future sales. Legitimate surveys destroy personal identifiers once data processed)
- 8:45 **Political canvasser at the door** (Political contributions of more than \$100—amounts and the party—are listed in public records)
- 9:10 **Log onto Internet** (Your choice of chat groups and your messages can be monitored and a profile assembled by anyone, including police; some Web sites monitor your visits); see *Privacy in Cyberspace* p.27.

Increasingly, living a modern urban life seems to mean there is nowhere to hide. In our search for security and convenience, are we hitching ourselves to an electronic leash?

Highlights

- Canadians' privacy protection weakening as government sells off operations with no binding privacy clauses (page 1);
- Under construction: permanent voters list—some warning markers around the potholes (page 14);
- Violent offenders in the community—is publicity the answer? (page 22);
- Privacy in Cyberspace—tips for surfers (page 27);
- A framework for introducing multi-function smart cards (page 8);
- 1681 complaints investigated, more than 9000 inquiries handled (page 33).

Table of Contents

Mixed Messages	1
Of Ethics and Smart Cards	6
Building a DNA Database—Carefully	12
A Vote for Privacy?	14
And the Walls Come Tumbling Down	17
This Year's Telecom News	20
One Size Does Not Fit All	22
Refining the Criminal Records System	25
Privacy in Cyberspace	27
Canadian Institute for Health Information	30
Update - The Privacy Patchwork	32
Investigating Complaints	33
Inquiries	40
Tables and Charts	42
Monitoring Compliance	47
Audits	51
Follow-ups	54
Information Sharing Study	56
In the Courts	60
Taking the Show on the Road	61
Corporate Management	63
Organization Chart	65

Mixed Messages

"Necessity is the plea for every infringement of human freedom. It is the argument of tyrants; it is the creed of slaves."—William Pitt the Younger, 1793.

The great British parliamentarian's words, uttered more than 200 years ago, have never been more relevant, timely or applicable than they are in today's struggle to hang on to our right to a private life.

Society, in the throes of an unparalleled technological revolution, is confronted daily by arguments that yet another infringement of our personal freedom is necessary, the usual necessity being those seductive benefits: efficiency, convenience and economy. Sometimes the benefit is real; sometimes it is merely promised, not proven; often it is mostly for the efficiency, convenience and profit of its proponents.

Yet if there is a tyrant, it is not some jackbooted dictator. It is the tyranny of ignorance, of unthinking acceptance of technology without regard to the consequences. The tyrant and the slave are one and the same. It is ourselves.

A Backward Leap

Sadly the struggle—thought to have been largely won in the public sector—suffered a body blow this past year. Thousands of Canadians lost their rights under the *Privacy Act* as the federal government began downsizing and privatizing. Information previously collected by government entities will soon be moved from under the protection of the *Privacy Act* and into the control of private companies. This means that innumerable bits of personal data no longer will have to be managed in accordance with fair information practices; the subjects of all this information will have no legal right of access to the information and no legal control over what information is collected about them, how it may be used, disclosed or otherwise disposed of.

Most immediately, commercialization affects the thousands of federal government employees who are transferring to the private sector. But equally important, it touches the untold numbers of Canadians who use services previously managed by government.

This constitutes nothing less than a privacy disaster, and is a dark stain on the otherwise progressive record of the Canadian government in protecting Canadians' privacy rights. This consequence of privatization may have been entirely unintended; it can hardly have been unforeseen. And, regrettably, it was entirely preventable.

The issue arose in dramatic fashion during the transfer of the air traffic control system to a private company, NAVCANADA. An estimated 6,000 federal employees will move from government to private employment. As well, the air traffic control system generates substantial personal information in its contacts with thousands of users of the system.

Given the magnitude of the transfer, the Commissioner wrote to the government last November pointing out the consequences to privacy protection and offering a solution. He suggested inserting a condition to the agreement between the government and NAVCANADA making the company subject to the *Privacy Act*, as it is subject to the *Official Languages Act*.

Although the government conceded the importance of the issue, it took no action. The Commissioner then appeared before the Commons Transport Committee studying the transfer. The committee accepted the proposal and recommended it to the House of Commons. The government objected to the recommendation and, despite a further intervention before the Senate committee, the bill has now cleared both Houses with no privacy protection.

Among the objections put forward both by NAVCANADA and the government, foremost was the contention that binding NAVCANADA to the *Privacy Act* would single it out for special treatment by a government which otherwise has not enforced privacy law in the commercial sector. There is ample precedent.

It is government policy to recommend that contracts between government departments and outside service providers contain clauses extending *Privacy Act* protection to any personal data. Furthermore, at least one huge enterprise, Canada Post, was required to abide by the *Privacy Act* when its corporate structure was revamped and its mandate altered to make it operate in the manner of a private sector, profit-and-loss corporation. Although owned by government, Canada Post must compete in the open market for much of its business. This is not a problem NAVCANADA, a monopoly, will ever face.

Whatever one makes of these arguments, the government has an obligation not to sacrifice basic rights such as privacy and data protection as it commercializes operations, particularly when the available defence is as simple as insisting on a privacy clause. It is worth pointing out that one of the chief government negotiators publicly stated that *Privacy Act* protection would not have been a "deal-breaker".

As for the company, NAVCANADA has undertaken to seek employees' consent for transferring personal files and to keep the records confidential "pursuant to government policy". Fine words but not ones that convey any legal rights, and far from the protection they now enjoy. The Office intends to audit the personal records before Transport Canada transfers them to NAVCANADA.

Canada's air traffic control system is simply one of several operations to be commercialized. Next on the block is Canada Communications Group, the government's massive printing, distribution and inquiries operation. Already gone are the harbours and many airports. And in the works are a new breed of "service agencies" to provide selected services of existing government institutions. These include Parks Canada (formerly Environment Canada), a single food inspection agency (Agri-Food Canada) and the Canada Revenue Commission (Revenue Canada). These new agencies will be given greater autonomy to improve service and reduce costs and have more flexibility to allow provincial participation. At issue is whether "streamlined rules and flexible authorities" and separate legislation also spell the end of privacy protection for clients and employees.

"Twixt Darkness and Dawn"

The light at the end of this murky tunnel may be the news contained in the government's response to the recommendations of the Information Highway Advisory Council. Perhaps saving the best for last, Industry Minister John Manley announced the most important privacy development of recent years, and potentially the most important in Canadian history: the federal government's commitment to introduce legislation bringing the commercial world under the ambit of privacy laws.

The report, *Moving Canada into the 21st Century*, acknowledges that when it comes to protecting personal information in an information society, "security procedures and technologies cannot do the job alone. The right to privacy must be recognized in law, especially in an electronic world of private databases where it is all too easy to collect and exploit information about individual citizens".

The ministers of Industry and Justice undertook to consult with the provinces "and other stakeholders" and bring forward proposals for "a legislative framework governing the protection of personal data in the private sector".

Here, at last, is at least the prospect of meaningful action.

To meet the threats to privacy posed by the information revolution, nothing equals the need for bringing order, fairness and decency to the information

management practices of the private sector. This is where most personal information is collected and used, and this is where there is the least protection for, and recognition of the rights of individuals.

The government, in developing this framework legislation, has the opportunity to build on what may be a growing consensus for action. One early indication of support came in the Canadian Direct Marketing Association's brave announcement of support for legislation to protect personal data in the private sector. In CDMA President John Gustavson's words "legislation is the most effective means of ensuring all private sector organizations adhere to the same basic set of rules...". And the trail has already been substantially blazed by the Canadian Standards Association's now-final model privacy code. The code was drafted with major private sector players such as the banks and telecommunications companies and contains all the essential elements for good privacy protection save independent oversight and the force of law.

Mr. Manley's announcement included no details, for the good and obvious reason that the work is just beginning. As usual, the devil is in the details. The government can bring forward truly effective legislation, heralding a new dawn in which technology follows a path lighted by civilized standards of respect for the rights of human beings. Or, if the action is excessively timid or, as is so often the case, the bold initial thrust is emasculated by concessions to special interests, we will find ourselves mired in the grip of ineffectual patchwork laws with little ahead but a gathering gloom of greater surveillance and less control over what others know about us. Such an outcome would be worse than no action at all, deluding us, as it would, with a mere illusion of protection.

So Canadian society finds itself at a critical point, where its privacy is poised between salvation and sinking. Everything now depends on the will and creativity of governments and Parliament.

Toward a new birth of civility

Although we have placed great emphasis on the need for better privacy laws, laws alone are not the answer. They are merely the written expression and refinement of a social consensus of fundamental dos and don'ts—those ethical principles on which we build common values and our individual and collective behaviour. Breathing life into our laws demands a climate of broadly-accepted ethical principles, a sort of ethical glue. It is time we took a hard look at the ethical issues raised by new technology.

Any casual perusal of the daily press demonstrates that our ethical glue is losing its sticking power. Look only at the chaos of hacking, unauthorized access into

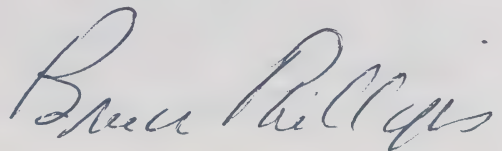
private and personal computer files, systems pranks and vandalism, software piracy, electronic harassment and bulletin boards of hate, pornography and violence. In short, technology has thrust us into the information age but we have arrived having given little thought to our social responsibilities.

We seem to suffer a stunning inability to put the pursuit of human dignity at the heart of our development and progress. It is not enough that new technology satisfy material needs. It must also play its part in affirming human dignity and human potential. Otherwise, we are conducting a technical exercise in a moral vacuum—moulding our lives to fit technology, not making technology fit our lives.

Social responsibility in the electronic world is everyone's business. It is maintaining the delicate balance between meeting legitimate information needs and simply respecting people, their property and their rights. We can no longer—if we ever could—afford to do things simply because we have the technical capacity. We must dedicate time and resources to the process of discerning ethical dimensions and integrating ethical decisions into the technology design process. We must educate young people about the rules of morality, civility and mutual respect in cyberspace. Our enthusiasm and expectations will be pointless if we simply become more technically adept but not more learned, thoughtful and considerate. In short, we must build an ethical foundation for technology.

It all comes down to the degree to which we respect one another as unique individuals, each with our own set of values, which we are entitled to conceal or reveal as we choose. To truly respect your neighbour, you must grant that person a private life. The limits of our personal privacy define in large part the limits of our freedom. As Supreme Court Justice La Forest put it in a 1990 decision "...not to be compelled to share our confidences with others is the very hallmark of a free society". If we discard the notion of privacy and simply treat one another as data subjects, as objects of surveillance, we abandon that fundamental, democratic notion of autonomy and self-determination.

Let us be clear. No amount of information or technology will do much good unless we consider the values it serves.

A handwritten signature in dark ink, reading "Bruce Pillsbury". The signature is written in a cursive, flowing style with a large initial 'B'.

Of Ethics and Smart Cards

ID card stories are standard fare for Privacy Commissioners' annual reports. This year's menu is rich. Governments' appetite to cut spending, simplify and privatize program delivery, and to ferret out cheats, has led to a plethora of proposals most of which are supported by new, glitzy technologies.

The key component of these proposals is often a multi-purpose ID card or a smart card which looks like the pieces of plastic found in most wallets. However, imbedded in them are powerful microchips and circuitry which allow the collection, storage and manipulation of vast amounts of data. The cards can be inserted into electronic readers and operate like a personal computer plugged into a network. They are low cost, versatile, simple and powerful; hence their attraction. They are yet another intriguing new option for bureaucrats and private sector administrators to deliver programs more efficiently and more cheaply for our benefit and their profit. As journalist John Ibbitson described them in a recent *Ottawa Citizen* article, they are fast becoming a "plastic panacea".

Improperly applied, these technologies can be powerful surveillance tools, delivering the fatal blow to an already fragile and embattled right. Those who consider the fears exaggerated need look no further than the quoted words of the Ontario Cabinet Minister on Ontario's plan to introduce a multi-purpose smart card. This proposed card would replace existing driver's licences, health and welfare cards and keep a timely record of citizen's use of the system " ... like Visa or Mastercard where they can tell you where you were an hour ago and how much you spent, that would be a great step forward for the health system in Ontario". Perhaps a great step forward for efficient administration of the health care system, but certainly a giant leap backwards for autonomy and privacy.

Toronto's welfare card

An example of the efficiency and the surveillance capacity offered by smart card technology is the Metro Toronto proposal for welfare recipients to carry cards containing a digitized fingerprint. The fingerprint is not a conventional inked impression but a picture transformed into an encrypted numerical code (known as a "biocrypt"). Welfare claimants would be required to produce their cards to claim a service. A reader will scan the biocrypt to ensure it matches the code imbedded in the card. The system allows the code to be stored only on the card thus allowing the claimant to retain control.

The downside is that welfare payments could be credited to a card which can then be used for direct debits at stores. While it is clear the present proposal will not track the behaviour of people, it would be a simple matter, once implemented, for the system to collect information about the life styles and the spending habits of welfare recipients. There is an added human cost which is to require a segment of the population to be monitored in a way, usually reserved for criminals, that no other citizens have to suffer. The data may also prove to be attractive to social science researchers. Officials estimate that the cards will save \$32-million from the annual \$1.1-billion cost of operating the welfare system by eliminating claimants collecting more than one cheque.

A similar proposal in B.C. using laser photo smart cards would merge drivers' licences, welfare cards and health cards. B.C. Privacy Commissioner David Flaherty termed the proposal an invasion of privacy, and the B.C. Civil Liberties Association considered it acceptable only if used for identification purposes.

The SmartHealth process

The prairie provinces have all considered switching to smart card technology to deliver health care services, hoping that stricter monitoring and control of patient claims and health practitioners' billings will lead to savings. One early example is Manitoba's proposal for a Health Information Network to exchange patients' health care information throughout the health care system and make it available for research. The province awarded a contract to SmartHealth, owned by the Royal Bank of Canada, to examine the proposal.

Manitoba's approach illustrates how best to use the technology; first define the needs and then look for the technology solution. SmartHealth conducted numerous focus groups, surveys and interviews and found "among the most cited concerns were fears of personal health information falling into the wrong hands". Manitoba has concluded that privacy safeguards must be in place **before** the network is developed; it will then select the most appropriate technology for the task. A smart card is simply one of the options.

However, Manitoba's proposal also illustrates what is a growing (and potentially alarming) trend to deliver government services in partnership with the private sector. Personal information now largely protected by privacy rules will be shared with the private sector which is subject to no privacy laws and increasingly anxious not to be. Private sector "opting in" to voluntary privacy codes is a grossly inadequate trade-off for gaining access to data and transactions which now have legal protection.

There is also a ray of hope in a Québec proposal to introduce smart card technology as part of the government's information highway strategy. Like other provinces, Quebec's multi-purpose smart card would replace existing government identification cards. Unlike some other proposals, however, the Québec card would be used for all program delivery, including such things as hunting and fishing licences. The most important difference lies in the government's stated intention to measure technological initiatives against three fundamental principles: universal and equitable access, privacy and the confidentiality of personal information, and respect for existing social values.

The project could well build on the province's experience with a pilot project to introduce a health smart card in Rimouski. In his report on the pilot project, Quebec Privacy Commissioner Paul-Andre Comeau observed

"...the success of the project (was) due first and foremost to the guarantees of confidentiality offered by project designers and the choice of a technology able to ensure confidentiality...".

Smart cards have the potential to destroy our privacy or to enhance it. We can use them as a powerful surveillance tool to monitor and control individuals; or we can use them, not only as a device to protect the security and confidentiality of our personal data, but also as a device that will allow us to exercise a greater degree of control over uses and disclosures of our personal information. Should our lives fit technology or technology fit our lives? Ultimately the choice is ours.

A Privacy Framework for Smart Cards

The *Privacy Act* sets out the ground rules for federal government collection, use, disclosure and protection of personal information and establishes a commissioner as independent oversight of government compliance with the law. Since smart cards are potentially major data collection, storage and disclosure tools, the Office proposes a framework to ensure that government institutions take privacy and other ethical principles into account in the applications design phase of smart cards. We welcome readers' comments and suggestions.

Is the collection related to a government program?

The *Privacy Act* requires that government institutions collect no personal information unless it relates directly to an operating program or activity.

Regulatory/legislative framework: To show a direct relation to an operating program or activity, an institution must ordinarily demonstrate that it has Parliamentary authority to collect the information. Thus, some legal mechanism (legislation or regulation) should govern each smart card system whether for client services or program delivery. These should specify

not only the technical and administrative characteristics of program delivery but also the ethical codes which will govern privacy, confidentiality and security.

Is the information collected directly from the individual and he or she notified of the purpose?

The *Privacy Act* generally requires that personal information be collected directly from the individual and the individual informed of the purpose for collection.

Public notice of systems: In the broadest sense, government should alert the public to the system's development—for example, its objectives, extent, the type of data and clients affected—before the system is implemented.

Individual written notification: The government should provide each card holder, in writing, the essential information about program participation and use of the card. This includes details about the purpose, nature, operation of the system, contents of the card, and the individuals authorized to access it (either read or record).

Government should also inform card holders of all possible communications between the issuer (the government agency) and the card users (the service provider/point of delivery of that program).

How long will the information be kept?

The *Privacy Act* requires government to prescribe retention spans for personal information.

Data conservation: Card issuers and users must establish retention and disposal schemes for data. Issuers should establish regulations governing the nature of information conserved and the security measures taken to guarantee confidentiality of the data.

How will accuracy of the information be ensured?

The *Privacy Act* requires a government institution to take all reasonable steps to ensure that personal information is as accurate, up-to-date and complete as possible.

Responsibility for inaccurate information: Card users should not automatically accept the accuracy of the information simply because it is recorded on the card—the data could be false, incomplete or obsolete. Accuracy is a joint responsibility of the card issuer, card user and card holder.

How will the information be destroyed?

The *Privacy Act* requires that disposal of personal information be regulated to ensure the data can no longer be used or improperly disclosed.

Card renewal: Government must establish which data from old cards should be transferred to the new card; and whether old data should be rendered anonymous and available for research purposes.

Destruction of the card: Subject to the regulatory authority governing destruction of the card, individuals should have the right to request that the card be destroyed; this would include rendering anonymous all data stored by the card issuer about the card and its contents.

How will the data be used and disclosed?

The *Privacy Act* sets out principles of fair information practices governing how personal information may be used or disclosed.

Reading the card: Government must determine who it will authorize to read the card, the extent of authorization (total or partial), and the protocols governing the reading function.

Restricting reading access or use for other purposes: Government must establish conditions and measures to prevent unauthorized access to card files or uses other than those originally intended. Access must be restricted only to those who have an authorized need-to-know under the *Privacy Act*.

Restricting unauthorized use, disclosure and copying: Government must institute proper controls to prevent card users from unauthorized downloading of information from the smart card to other databases and then using it for purposes unknown to the card holder.

All non-government card users or readers must operate under regulatory restrictions by agreement with the government program authority and have no automatic rights to copy other data from the card—this must be subject to the card holder's authorization.

Card structure: The card chip should be structured in different zones of access to assure selective or limited degrees of access as well as segregation of identification data, administrative data, and sensitive data such as medical or emergency help information.

Government should segregate each application on the card to prevent merging or cross-overs of data. Readers and public point-of-delivery devices must secure transactions to and from the host computer.

Individual authorization for reading access: The file contents of the card shall not be accessed by third parties except by a positive act of the card

holder (or by the card holder's authorized agent, as in a medical emergency). Such positive action would generally be punching in a PIN or other code.

Entering/removing information on the card: Government must determine who may enter, change or delete data on a card, either directly or through the delivery authority. Issuers must consider the individual's right to demand erasure of parts of information on the data card from every institution that makes entries.

Visible data on the card surface: The card exterior should contain only the minimum amount of nominative information required for the purposes of program participation.

Do individuals have right of access to the personal data?

The *Privacy Act* gives individuals the right of access to personal information about them.

Transparency of data on the card: Individual card holders must be able to know the type of information held on the card.

Right of card holder to read the file: Government should provide individuals the means to read their own cards. They should also be prepared to interpret the data for card holders.

Data entry/transaction record: Card issuers and users must compile and maintain a record of all significant data entries as well as all communications between them concerning the card holder. These records should also be available to the card holder.

This suggested framework is based on the privacy checklist for technology set out in the Commissioner's 1992-93 annual report (see page 14).

To obtain copies of the complete text of the *Privacy Framework for Smart Card Applications*, or to submit your comments, please contact the Office or visit our Web site.

Building a DNA Database—Carefully

Last year we reported our recommendations on the proposed bill to allow police to obtain DNA samples from a person suspected of a serious crime. The law was enacted in July 1995.

However, the legislation did not deal with several privacy issues, the most important of which was whether to establish a database of genetic samples or analyses derived from those samples. Early in 1996, the Solicitor General issued a consultation document, *Establishing a National DNA Databank*, that dealt with many of the remaining privacy issues. Our response made several proposals:

- samples should be taken for the database only after the person has been convicted (as opposed to samples taken during an investigation to prove the crime in question). For the "less serious" of these serious offences, a judicial warrant would be needed to acquire the sample for the database. For the more serious offences, taking the sample would be automatic;
- once the analysis of a sample appears on the database, either automatically or by judicial warrant, the police should be permitted access to the database whenever they have DNA evidence from a crime scene that may match a sample taken for the database;
- only the forensic analysis of DNA samples taken from convicted offenders should be kept, not the actual samples. Discarding the actual samples would prevent unrelated secondary uses, including ethically problematic research into genetic links to crime;
- volunteered samples for a criminal investigation (for example, when the police appeal to a community to volunteer DNA to help track down a violent criminal) should be used only for the investigation of the offence in question; the samples and the analysis of the samples should be destroyed immediately after the donors are exonerated;
- DNA identification information on the database should not be kept indefinitely. It should be destroyed when it is no longer needed—for example, after the offender has died or after sufficient time has passed (perhaps decades in some cases) and the offender is not likely to reoffend;
- legislation establishing a DNA database should provide for a review of the database operation within two to three years of the legislation coming into force. The review would include a privacy audit.

The privacy audit is particularly important. Two or three years experience with the database should give a good idea of its utility in solving crimes. It will also

help to ensure that the database does not become subject to "function creep". We want to avoid an ever-lengthening list of offences for which a DNA database or DNA sampling in criminal investigations is allowed. The pressure to do just that is already present in our society, a product of the very existence of technology and the belief that technology can solve all our woes, if only we let it.

Legislation dealing with these remaining aspects of forensic DNA analysis has yet to be introduced in Parliament. We await any such proposed legislation to ensure that it meets our criteria.

As a final note on this subject, we commend both the Department of Justice and the Ministry of the Solicitor General for recognizing privacy issues as among the most significant in the discussion of forensic DNA sampling and DNA databases. We also commend them for involving our office in the consultation process *before* legislation is introduced. Their willingness to discuss the privacy issues with our office ensures a hearing at a time when changes can be accommodated with little political embarrassment.

A Vote for Privacy?

Canada's Chief Electoral Officer recently proposed amendments to the *Canada Elections Act* which would give him authority to create a permanent voters register. The notion is not new. It was considered, but not recommended, by the 1991 Royal Commission on electoral reform. Canadians have traditionally resisted such proposals because population registers pose a potential threat to human rights and freedom. Wartime memories are etched in the minds of many.

Political climates change, however. In the age of "fiscal responsibility", what was previously unacceptable is now fashionable on condition that millions of dollars can be trimmed from public expenses. Québec and British Columbia have recently created permanent voters registers citing budget reductions and efficiency. The federal government now proposes to follow suit. "Efficiency, economy and accuracy" is the rallying cry; there are other equally important considerations.

The proposal

Elections Canada proposed to create the permanent register from one last traditional door-to-door enumeration. Enumerators would collect the name, address, sex, date of birth, telephone number, and confirm citizenship of potential voters. The Chief Electoral Officer would also have the authority to collect additional information if necessary. Once collected and validated, the data would be stored in an automated database. Individuals would not have to register and could have their names removed at any time.

Elections Canada also proposed to conduct periodic data matches with other government data bases such as tax and motor vehicle records to update addresses; with vital statistics to remove the names of deceased persons; with citizenship records to add new Canadians entitled to vote, and with provincial election lists after elections to update the data.

Provinces, municipalities and school boards could obtain information from the register to conduct local elections. And every year all members of Parliament would receive the list of voters in their respective constituencies.

The response

It is both laudable, and consistent with existing *Privacy Act* rules, to begin by direct individual enumeration. This gives citizens the opportunity to decide whether to be included on the list and to provide the information directly. However, there are several concerns.

Telephone numbers The Office questioned the proposal to collect a new data element—telephone numbers. Telephone numbers are not needed now and their appearance on a voters' list would seem to beg intrusive calls. Elections Canada explained that the numbers will be used only for internal administrative purposes and will not be included on the lists.

Power to collect more data The provision allowing the Chief Electoral Officer to collect additional information aroused some early concern, opening the door—as it seemed—to a broader collection than legislators may intend. The provision is simply to permit the federal agency to collect additional personal details if required by provincial election laws. The Chief Electoral Officer undertook to make this clear in the legislation.

Annual disclosure of lists to legislators Annual disclosures of the list appears excessive in light of the list's express purpose of conducting elections or referenda. Given that no jurisdiction conducts annual elections, this frequent a disclosure seems more suited to repeated canvassing by political parties, not the election itself. The Chief Electoral Officer agreed to re-examine the need for annual disclosures.

Collection by data matching Updating the register by data matches with other federal data banks is worrisome. On principle, the Commissioner opposes mining other government databases for unrelated uses. Datamatching is invisible and inconsistent with the federal *Privacy Act*. The preferred method is for Elections Canada to collect the information directly from the Canadian public, with their knowledge and consent.

The Commissioner suggested that Elections Canada arrange to include a consent box on other federal government forms to authorize departments like Revenue Canada or Human Resources Development Canada to transmit the personal data. British Columbia uses this system to maintain its electors' register. Or Elections Canada could develop a specific form to be enclosed in all government mailings and returned directly to Elections Canada. The Chief Electoral Officer undertook to pursue the idea.

Other uses of the list By far the greatest concern is pressure for secondary uses of the register. It will be a very attractive list of the majority of Canadian citizens and hold enormous potential for any number of public organizations. Other levels of government which have created permanent registers have found that requests for access by other government programs soon follow. These are difficult to resist. Growing authorized access to Revenue Canada's list of tax

filers—once virtually off-limits—leads one to suspect that the voters' register will soon be targeted.

The Chief Electoral Officer explained that requests for access to the list for any unrelated purposes—which the Commissioner would strenuously oppose—would require Parliamentary approval and thus be a matter for public debate.

The bottom line

The best conceivable privacy protection is resisting the temptation to administer a program by assembling vast amounts of personal information in an automated data base. If it is impossible to design an electoral process without such a collection—and Canadians accept the necessity of a permanent voters register—then the following conditions must be met:

- limit the personal information collection to those details needed for Canadians to exercise their right to vote;
- collect the information directly from citizens—with their knowledge and consent;
- limit uses of the register to those required for Canadians to exercise their right to vote, and
- prohibit disclosures of personal information from the register unless to conduct federal, provincial, municipal or school board elections—and then only where equal legal privacy protection exists.

And the Walls Come Tumbling Down

Early in 1994, Treasury Board Secretariat tabled its *Blueprint for Renewing Government Services Using Information Technology*. The blueprint responded to the federal government's call for a leaner and more efficient public service, encouraging every federal institution to use computer technology to streamline operations and eliminate inefficiencies.

Given the impact of several of the Blueprint recommendations on government handling of personal records, the Office asked to be involved in projects which federal institutions undertake. While more than 30 federal institutions have since begun re-examining their operations, two departments have taken a clear lead. Both have approached us for guidance.

Citizenship & Immigration Canada CIC's Business Process Re-engineering is the first major *Blueprint* initiative, one which other departments are viewing as a test project. CIC aims to become a "horizontally-integrated" work environment which means sharing more information about immigrants and refugee claimants both inside and outside CIC. CIC now segregates data according to its purpose or program (the vertical or "stovepipe" information environment common to most federal institutions). CIC has begun the transition to a horizontal environment which will integrate all its information resources.

Human Resources Development Canada (HRDC) is the other leader. HRDC is streamlining its delivery of employment insurance, Canada Pension Plan, workforce training and job bank programs and substantially reducing the number of Canada Employment Centres. HRD will deliver service to many communities by satellite and telephone centres, electronic kiosks, frequently in partnership with private businesses, Crown Corporations, special agencies or provincial and municipal governments.

The two initiatives illustrate two government trends and, if not properly planned, the risks they pose. They are data warehousing and shared service delivery.

Data warehousing

Perhaps the most significant development in government information management is the steady move toward departments developing so-called "data warehouses" to store and manipulate all their program data—including, of course, personal information used to make decisions about individuals. Human Resources Canada and Veterans Affairs Canada are just two of the institutions that are developing data warehouses.

A data warehouse is a sort of super repository which integrates data from a variety of sources, reconciles any anomalies, then makes it easily accessible for search, analysis and manipulation. Rather than segmenting the data by its intended use—for example, paying taxes, claiming Canada Pension Plan, or applying for a student loan—all the data is organized by the person's name and other personal identifiers. Find the individual and you have a record of all their transactions with the federal government.

For managers, the prospect is exciting. For privacy, it is troubling. Data warehouses, by definition, consolidate information thus making more details accessible to more people. Personal information collected for one purpose could become available for different and unrelated purposes.

And consolidation pushes demand for even more information—the data warehouse as insatiable appetite. This is what privacy advocates call "function creep". Warehousing data also permits the creation of client profiles—or more insidious—"client intimacy" systems drawn from historical transactions and relationships previously unknown.

Ultimately, the system demands a unique identifier to link to the individual's data file. Thus we arrive at the single number, single file, single card without which we are no-one. Like all advanced systems, the data risks becoming paramount, not the person; we are all reduced to bits and bytes.

Technological advances are undermining individual control over personal information. They may even be undermining privacy laws because protecting privacy becomes increasingly difficult as systems become more developed, more widespread and more complex.

That does not justify throwing up our hands. Nor does it justify the angry outbursts that privacy is the impediment to new systems development. The accusation that something cannot be done because of privacy is more often simply an excuse offered at the end of the systems development cycle; an attempt to assign blame elsewhere for not having done the work properly at the outset.

The accusation is simply wrong and short-sighted. Privacy does not restrict good systems design—it enhances it. Systems designers simply have to build in controls to limit employees' access to the data elements necessary to deliver the program or service. Privacy protection is an essential component of good information management and a good systems development plan; one which helps ensure public confidence in government's computer based systems. It's time to get on with it.

Shared Service Delivery

The second administrative trend with privacy implications is sharing service delivery points with other federal agencies, with other levels of government, and perhaps even private sector operators. The concept could be a boon to citizens—one-stop-shopping for municipal taxes, drivers' licenses, UI benefits and Canada Student Loan applications. But the privacy problems are evident. How will several levels of government protect the individual's records? Will the data and terminals be separate? Are the records under the "control" of the federal government, subject to the provincial privacy law or, if the centre is operated by the private sector—by contract compliance? Or will it be unprotected?

As with data warehousing, shared service delivery must be done with great care. If we are going to share services with provincial or municipal governments, we must make the obligations of various parties clear at the outset. And the answer is not sinking to the lowest level of privacy protection—in some jurisdictions, that is virtually none.

Much as the Office lauds federal government efforts to become more efficient, there are real privacy concerns with horizontal integration and shared service delivery. While our work with CIC and HRDC has allayed some fears, *Blueprint* initiatives may well create the unique on-line client file designed to be shared by federal, provincial, private or even foreign organizations who may need access.

Not only is this incompatible with the current *Privacy Act*, it raises the spectre of a surveillance society; one in which anyone will be able to learn anything about anybody. We have yet to confront two unavoidable realities: no computer system in the world has yet proven safe from hackers, and the weakest link in any computer system is the authorized users.

This Year's Telecom News

While technology may (and, occasionally, may not) enhance our quality of life, there is little doubt that it can have a dark side for privacy. Even its creators often do not fully understand the potential, let alone the users. Privacy is sometimes a victim of entrepreneurship, and this year's technological headline may again prove the point.

Personal Communications Systems

In December 1995 Industry Canada licensed four companies to offer Personal Communications Services (PCS). The small, hand-held devices, which can transmit voice, data, graphics and video, operate on separate frequencies from cellular telephones, relying on digital—rather than analog—transmission. Digital networks offer cheaper, better and more secure transmission and the increased ability to send text and images.

Given PCS marked improvement over cellular telephony, what is the problem? There are two of which Canadians should be aware.

First, PCS communications are still transmitted over the airways and so can be intercepted, albeit with more sophisticated and more expensive equipment. Second, PCS service must know your exact location at all times—at home, on the ski slope or in a shopping mall—to deliver calls. Unsettling enough, but its power to locate the user also makes it a tempting tool for criminals, law enforcement agencies, jealous spouses or direct marketers.

These two problems could be addressed by

- encrypting transmissions—this would provide sufficient protection for most users. Of course, encrypted communications can sometimes be deciphered, witness the recent breach of Netscape's Internet browser encryption algorithm;
- "locking" the handset so that the user requires a personal access code.

Industry Canada plans to limit the use of digital scanners, thus reducing the chance for interception of PCS communication. But another needed step is to prohibit PCS companies from either using or disclosing information about the subscriber's whereabouts for any purpose other than routing calls or billing PCS service. And PCS invoices should not display the exact location of a calling or called party.

Although the Canadian Radio-television and Telecommunications Commission (CRTC) does not now regulate PCS companies, it will hold public hearings later this year to determine which, if any, aspects of wireless telecommunications (including PCS) it will regulate.

If both manufacturers and regulators would safeguard the handset, the transmissions and the records, Canadians will reap only the intended benefits, not find themselves under surveillance from another piece of electronic wizardry designed to ease their lives

Other telecommunications news

De-regulating conventional telephone service has opened several cans of worms, some of these concern the right of competing companies to have access to the customer lists of full-service telephone companies. One immediate impact of disclosure of customer data to long-distance re-sellers was a blizzard of mail and marketing calls, and in some cases, clients being switched to other companies without their knowledge or consent.

The CRTC authorizes the full service companies to disclose their customer data to long distance resellers on request and with proof of the customer's interest. However, the re-sellers (which buy blocks of long distance calls from the telephone companies) are not regulated by the CRTC and some customers have been unaware of the switch until receiving their first bill. Customers can be returned to their original provider at no cost. More recently, private directory publishers have asked the CRTC for access to electronic client lists to publish directories, now published mainly by Tele-Direct, a Bell Canada subsidiary.

While the CRTC agreed that White Directory could compete against existing directory publishers, it ordered telephone companies to enable subscribers to remove their names and addresses from the electronic directory files before they were given to White Directory. White Directory appealed the "de-listing" mechanism to the CRTC, arguing that it would be at an immediate disadvantage because its directories would likely contain fewer listings than current directories, should many subscribers opt out. The CRTC upheld its earlier decision and White Directory filed a petition with the Governor in Council seeking to overturn the CRTC order.

The Privacy Commissioner supported the CRTC decision and urged to the Governor in Council to guarantee subscribers the right to full control over their personal information. The Governor in Council has up to one year to make a decision.

One Size Does Not Fit All

There appears to be a growing public outcry about releasing violent offenders into the community either on parole or at the end of their sentence. The concern is most acute with pedophiles. There is no doubt that some danger exists and Canadians have the right to try to minimize those dangers. An incident in Fort St. John, B.C. illustrates.

Fort St. John City Council, told that a known sex-offender was in the community, agreed to help local community groups print and distribute posters publicizing the man's presence. At a later meeting the Council resolved to pass on the information to other communities in B.C., Yukon and Alberta. The poster contained a photograph, physical description, list of convictions, as well as a notation about withdrawn charges. During the storm of publicity, the man left the community.

Both B.C. Information and Privacy Commissioner David Flaherty and this Office inquired—Dr. Flaherty into the actions of the municipality, and this Office into an allegation that the RCMP improperly disclosed information to the mayor of Fort St. John (information which actually appeared to be publicly available). Both commissioners concluded that while disclosure may be appropriate in some circumstances, the "shotgun approach", as Dr. Flaherty describes it, is often not the answer. Both agreed that a consistent national policy and process would help officials determine when disclosure is needed.

In an effort to shed some light on a heated discussion, the Office produced a discussion paper entitled *Publicizing the identity of violent offenders on their release into the community*.

Protecting the public from violent offenders is primarily the responsibility of the criminal justice system, mental health institutions and social welfare agencies. It is not usually a privacy issue. However, in part because the justice system is fallible and prison rehabilitation programs sometimes ineffectual, governments and the public look to other means of protection.

Is publicity the answer?

Publicity is becoming the cheap "solution" to a complex problem caused partly by structural weaknesses in the correctional system. Publicity also means governments are disclosing personal information about offenders without their consent. It is these disclosures that have drawn federal and provincial privacy commissioners into the debate.

Notifying the public about the presence of a violent offender may prevent further harm in some cases. However, publicity may actually produce greater harms:

- publicity may drive some offenders underground and away from treatment, making them more dangerous;
- publicity may give the community a false sense of security that all dangerous offenders have been identified, when in fact most likely have not;
- publicity may make it impossible for a released offender to remain in a community, thus hurting chances for successful reintegration into society;
- since many violent offenders will not reoffend, disclosing information about them may unjustifiably harm them; and
- unwarranted publicity may threaten the physical safety of offenders, often with no consequential benefit to society.

From a privacy perspective, any measures that warrant breaching the offender's privacy should have a demonstrable public benefit. If there is no benefit, there should be no disclosure. Two questions need answering: When is it appropriate to release personal information about an offender who has left an institution on parole, under statutory remission, or at the end of the sentence? Who should have authority to release the information, and to whom?

The discussion paper examines several possible disclosure programs for releasing violent offenders into the community. Among them are those used in B.C. and Manitoba. Both programs involve the interested parties—police, correctional officials and, in Manitoba, public interest groups—in examining the circumstances of an offender and then deciding whether disclosure is warranted and if so, to what extent.

Privacy Act does not prevent release

All too often officials claim that the federal *Privacy Act* prevents them from releasing personal information that would identify a pedophile or other dangerous offender in a community—even if it might serve the public interest to do so.

This is not so. The *Privacy Act*'s prohibition against disclosure of personal information may be overridden if the head of the government institution concludes that there is a demonstrable public interest. The head must then notify the Commissioner's Office. Staff examine the circumstances leading to the disclosure proposal and the type of disclosure. The Commissioner then decides

whether to notify the individual about the disclosure; however, the Commissioner has no authority to stop the release.

To repeat this oft-misunderstood point: The Privacy Commissioner has no power—other than that of persuasion—over releasing information about a potentially dangerous offender to the public. The Privacy Commissioner neither initiates or prevents the release. If anything, the *Privacy Act* provides rules to facilitate the release of personal information in the public interest.

Striking the balance

There is no easy solution to these complex issue of protecting society against dangerous human behaviour. To determine whether disclosure may help to resolve the problem, we recommend establishing a process to assess the factors. Among the factors that need assessing are the risk that the person will re-offend, the ability of measures other than publicity to reduce the threat, the possible harms that may flow from publicity—both to the community and the offender—and the extent of any publicity that is warranted.

The schemes used in B.C. and Manitoba appear reasonable models for striking a balance between the public interest in knowing the presence of a potentially dangerous person and that person's right of privacy. Our discussion paper offers tentative support for such schemes for any offender who poses a certain level of risk of serious violence to the community, not merely sex offenders. For provinces that do not have such schemes, a federally appointed government/lay committee could make recommendations to the RCMP, Correctional Service Canada and the National Parole Board about disclosure in the public interest.

Copies of the discussion paper will be available from the Office and on our Web site.

Refining the Criminal Records System

A criminal history records system is a vital tool for police forces and other agencies which investigate and prevent crime. This powerful and sensitive record collection is maintained by the RCMP in its information bank CMP PPU 030, Criminal History Records and Identification Fingerprints. The database is subject to the *Privacy Act* and during the past year Office staff completed a study of its contents and administration.

The study helped dispel a number of misconceptions that had developed about what information is contained in criminal history records and how it is managed. The RCMP is aware of the sensitivity of this personal information, of the need to ensure it is accurate and up-to-date, and of its responsibilities to properly manage the information. Interviews with members of the RCMP and other police forces helped confirm that the RCMP makes every possible effort to ensure the information is accessible only to individuals and organizations who need to know.

Although the RCMP's overall management of the information continues to respect the *Privacy Act*, staff identified several opportunities to strengthen compliance. They include the following issues:

Mandate Although the study identified a number of pieces of legislation that refer to the RCMP's maintenance of criminal history records, neither Office or RCMP staff were able to identify a comprehensive authority. Since the information is used daily by police agencies and other organizations to make significant decisions about individuals, specific legislation or amendments to existing legislation would better serve the interests of both the RCMP and the Canadian public. The legislation should spell out what information may be collected, how it may be used and to whom it may be disclosed.

Content of Criminal History Records The current definition of criminal history includes not only charges for which an individual has been convicted, but also charges stayed, withdrawn or for which the individual was found not guilty. Although information about charges for which an accused was not convicted can be valuable to police forces, it should be held in a separate information bank to which access is more limited. This would ensure it would be available only for authorized police investigations and not for such other uses as screening employees. Since the 1987 Ministerial Directive on disclosure of criminal history information is being revised, the time seems right to consider creating a second bank for records for which there was no conviction.

Cessation of Pardon The *Criminal Records Act* provides the National Parole Board with the power to revoke a pardon after giving the individual an opportunity to make representations.

The Act also provides that a pardon ceases if an individual is subsequently convicted of an indictable or hybrid offence. In these cases, the Act requires the RCMP to restore all entries concerning the pardoned offences into the regular criminal records system. The individual has no opportunity to make representations or to be advised that the pardon has ceased. This may lead the accused to believe that information once inaccessible because of the pardon, is once again available for use against the individual.

The RCMP should modify its procedures to include notifying the individual, whenever possible, that pardon has been revoked, thus making the system much more open to everyone concerned.

Info Source Description The RCMP's criminal history records do not always contain an individual's complete criminal history because police and correctional agencies are not obliged to provide information to the system. The bank description in *Info Source* is unclear and could lead readers to conclude that the bank is a complete history of all criminal charges and convictions. The RCMP should amend the bank description to describe the information more accurately.

Printed copies of the *Study of Criminal History Records Maintained by the RCMP* can be ordered from the Office or obtained from our Web site.

Privacy in Cyberspace—a surfer's guide

At last count (or best guesstimate) 40 million people worldwide are surfing the Net for fun and profit. Surprisingly, many of them are simply unaware that their communications, transactions—and perhaps even the data on their own computer—are available for others to see (unless they take precautions).

The openness of the Internet should not be surprising—the Net evolved from a U.S. Defence Department communications network (ARPANET) linking military bases, university research centers and defence contractors. It was designed to be open and accessible—to communicate and to be impervious to nuclear attack. Other computer networks and universities quickly joined.

Today the Net is multiple networks with many pathways connecting many computers. Messages can be routed around the world to reach across town and seldom travel the same route twice. The Net resides nowhere and everywhere; it has no headquarters and no-one is "in charge". That is its power—and its challenge to privacy.

Sitting quietly in front of our personal computers, it's easy to be lulled into forgetting that sending E-mail is not like making a telephone call; it's more like broadcasting. We should have few expectations of privacy. In fact, not only are our messages to public newsgroups or forums accessible to others, software available on the Net allows others to assemble a profile of our messages and interests. Soon marketers will systematically mine the Net to assemble personal profiles and target lists to sell products and services on line. And shopping and banking over the Net pose their own risks unless the service is protected by encryption.

The power and reach of the Internet gives users and system operators extraordinary access to data, including personal information. In January 1989 the Association for Computing Machinery (ACM), recognizing the social impact of their profession, drew up a code of ethics to articulate members' responsibilities. One of these is to "respect the privacy of others".

But, given the nature of the Net, individual users must also take responsibility. Here, then are some suggestions for protecting privacy in Cyberspace, adapted with their permission (and our gratitude) from a fact sheet of the Privacy Rights Clearinghouse at the Centre for Public Interest Law, University of San Diego, California.

- **Create a secure password** Make up something nonsensical from a combination of upper and lower case letters, numbers and symbols, or something no-one could guess; a combination of family names, birthdates or interests.
- **Ask for your system operator's privacy policy** Most commercial services have written policies which they provide to new subscribers. Avoid those that don't. Read carefully all messages which appear at initial login; many "sysops" inspect e-mail and require new subscribers to allow e-mail to be monitored.
- **Shop around** Investigate new services before you use them. Post a question in a dependable forum or newsgroup. If others have had a bad experience, you will hear quickly—news gets around in cyberspace.
- **Assume your communications are not private** Unless you encrypt, do not send sensitive personal information (phone numbers, passwords, addresses, credit card numbers, vacation dates, social insurance numbers) by chat lines, forum postings, e-mail or in your on-line biography.
- **Be cautious of "start-up" software** Programs which make the initial connection to a service may ask for your credit card number, chequeing account numbers, Social Insurance Numbers, then upload the information automatically for billing purposes. These programs may also be able to access records in your computer without your knowledge. Ask the service for alternate subscription methods.
- **Don't leave footprints** Use anonymous remailers to avoid leaving tracks of your logins and the commands you executed both at your service provider and remote sites.
- **Remember the "Delete" command doesn't...make your messages disappear**, that is. They can still be retrieved from back-up systems and your hard drive.
- **On-line identities may not be what they seem** Many network users adopt one or more on-line disguises.
- **Avoid listing sensitive or controversial newsgroups as "favourites"** If your on-line service allows you to compile a list of favourite newsgroups, avoid listing those with which you do not want to be publicly identified.
- **Take care creating your on-line biography** If you need to protect your identity, don't create a biography, and ask the operator to remove you from its on-line directory. Biographies may be searched system-wide or "fingered" remotely.

- **Setting up a personal Web page makes you a marketing target** This seems self-evident, but it's often forgotten.
- **Be alert to social dangers** Harassment, stalking, being "flamed"—subjected to emotional verbal attacks, or "spammed"—sent repeated unsolicited messages, are all possible on the Net. Women can be particularly vulnerable; use gender neutral on-line IDs.
- **Teach your children well** Make sure your children also learn the privacy lessons. Caution them against revealing information about themselves or your family.
- **Use privacy protection tools** If you are concerned, consider using technologies which help on-line users protect their privacy. These are:

Encryption: these scramble e-mail messages or files, making them gibberish to both the system operator and anyone other than the intended recipient. Various encryption programs (such as PGP—Pretty Good Privacy) are available on-line;

Anonymous remailers: these servers act as intermediaries for your message, stripping off the identifiers before forwarding the message;

Memory protection software: programs which prevent unauthorized on-line access to your home computer. Some include an "audit trail" to record all activity on your computer.

Canadian Institute for Health Information – a national medical record collection

The 1993-94 annual report discussed the privacy issues in a new national body set up to gather personalized medical data from provincial health institutions and transform it into aggregate statistical data for research. Since the Canadian Institute for Health Information (CIHI) is not a federal agency, the Commissioner was concerned about removing sensitive medical data from the protection of the federal *Privacy Act* (and even tougher *Statistics Act*) with no compensating safeguards in place. He offered any input that might prove helpful to ensure that sensitive medical data was properly protected. CIHI's initial response was tepid but the past year has seen a sea-change.

Background

Until 1994, provincial health centres provided information about individual hospital admissions, treatments and deaths directly to Statistics Canada and Health and Welfare (covered by federal privacy legislation), as well as to two non-governmental organizations, the MIS Group and the Hospital Medical Records Institute. These agencies rendered the personalized data into aggregate statistics and made it available for research.

A study by the National Council on Health Information concluded that the arrangement duplicated effort and produced overlapping responsibilities. The Council recommended integrating all the organizations' relevant activities into a single federally-chartered, non-profit organization with a mandate to create and maintain a completely integrated health information system for Canada. This is CIHI.

Midway through 1995, CIHI seized on the privacy issue and determined to draw up guidelines on protecting the vast store of sensitive personal data of which it is custodian. Senior CIHI staff sought the office's input; the result is four documents on privacy and confidentiality, one of which—*Privacy and Confidentiality of Health Information at CIHI*—sets out the guidelines. They include:

- 10 guiding principles governing collection, use and disclosure of personal information (based on the CSA Model Privacy Code);
- *Security and Privacy Guidelines for Health Information Systems* adopted from the Canadian Organization for the Advancement of Computers in Health (COACH);

- a data linkage policy modelled on Statistics Canada's Policy on Record Linkage, and
- a formal process for handling external requests for CIHI data.

These new guidelines will apply as minimum standards to all data under the control of CIHI. They will be implemented in 1996-97.

Two questions remain. One is unsettling; is it advisable to centralize so much sensitive medical information given the unprecedented power for surveillance and linkage its systems grant health bureaucrats? And notwithstanding the security systems in place, concentration of data increases the potential for information leaks.

The second question concerns the wisdom of CIHI piloting a national survey of some 22,000 Canadian households about their living habits, use of health services and their health problems. Previous health surveys were conducted under the stringent protection of the *Statistics Act* and the added safeguards of the *Privacy Act*. CIHI's guidelines are a brave statement of principle but they hold no power in law.

Update - The Privacy Patchwork

The past year was a quiet one for new privacy laws in Canada and abroad.

Alberta's *Freedom of Information and Protection of Privacy Act* came into force on October 1st. The law currently applies to provincial government records but will be extended to municipal and regional governments in the future. In November, **British Columbia** extended its *Act* to cover records of self-governing professional bodies such as the provincial College of Physicians and Surgeons—a first in Canada.

The **New Brunswick** legislature established an all-party committee to examine comprehensive privacy legislation to replace the province's current privacy code. Residents now have a legal right of access to their personal records but none to challenge the government's collection, use and disclosure of their personal records. **Nova Scotia** has begun reviewing its 1993 *Act* for possible amendment. **Prince Edward Island** remains the only province without any kind of access to information or privacy legislation.

Winnipeg appears to have broken new ground. In January, city council's new *By-law relating to Access to Information* came into force giving city residents rights of access to and correction of their personal information in city records (Manitoba's privacy law does not extend to regional and municipal governments).

Abroad, **Australia's** federal government is considering extending its *Privacy Act*, which applies only to federal records, to the private sector. In July the **European Parliament** ratified the *Directive* on data protection, which is now in force. Member countries of the European Union have until the summer of 1998 to adopt or adapt national privacy laws to comply with the *Directive*. Section 25 of the *Directive* prohibits member nations (and businesses within the country) from transferring personal information to a non-member country whose laws do not guarantee adequate protection of the information.

In the absence of nation-wide privacy protection laws covering both the governments and the private sector (except in Quebec), Canada may not meet the *Directive's* adequacy test and risks being at a trade disadvantage with other countries.

Investigating Complaints

The Branch's intake of new complaints levelled off at 1625 during 1995-96. Investigators completed 1681 cases, leaving 1630 open case files—virtually an entire year's workload—to be carried into the next fiscal year.

Two issues need highlighting in this report; both are the result of this huge backlog of complaints the Office continues to face.

Like virtually all federal government institutions, the Office is struggling with dwindling financial resources. But the combination of across-the-board percentage cuts and climbing caseload has pushed the Office to the critical point far more quickly than larger agencies. The Commissioner is funded only to investigate and cannot turn away—or charge—complainants.

Coupled with budget cuts are clients' increasing demands. Canadians demonstrate growing awareness of privacy threats, increased sophistication in framing complaints and a greater demand for respect for their privacy rights. More provinces have passed privacy legislation, there is a standard privacy code in the private sector, as well as a steady barrage of media stories about the dangers to privacy protection from technological advances.

The Office recognizes that it will cease to be relevant if it cannot respond to complainants in a timely fashion—justice is already being seriously delayed. To serve clients properly, the Office should have no more than 500 complaint investigations open at any time; about 35 cases per investigator.

The only option was to streamline the process substantially. In late 1995 the Office undertook an in-depth examination of its investigation process, including one-on-one meetings with staff in departmental privacy offices. The new process will reduce the paper burden, remove some of the formality, eliminate steps in the review process and allow greater reliance on the telephone—in short, a fast track approach to handling many of the complaints, one that builds on the strength and flexibility of the ombudsman role.

At the same time, the Branch implemented quality service standards aimed at reducing the time and effort required to investigate complaints, created a unit to focus on backlogged complaints, and another to concentrate on complaints about improper collection, use, disclosure and disposal of personal records (sections 4 to 8 of the *Privacy Act*). The Office will monitor the changes carefully, and fine-tune where needed.

Following are selected complaints from the year's caseload.

Three strikes—CIC out

Three times the owner of a Vancouver construction company returned packages of misdirected immigration files to the local Citizenship and Immigration Canada office. The fourth time, his patience ran out. He sent the file to the local Vancouver newspaper—the *Province*.

Apparently the Surrey CIC office had closed and the priority courier, unable to find a current address, continued to deliver packages (addressed to "CIC") to the nearest likely destination—CIC Construction in West Vancouver.

The journalist called the Vancouver CIC office. The manager reacted immediately, retrieving the file, calling the Montreal office to correct the address, and then the courier service which traced the deliveries. The courier acknowledged that the packages should have been returned, or instructions sought from the sender. The manager agreed to be interviewed and photographed but asked the journalist not to identify the subject of the file in the article. The journalist agreed but had already called the man for his reaction to the disclosure and asked him about his immigration status. Understandably upset, the man complained to the Commissioner.

It was obvious that the immigration file (which contains photographs, fingerprints and sworn statements about his political background and reasons for seeking refuge in Canada) had been improperly disclosed. Despite three earlier opportunities, CIC had failed to determine why files were being returned or take proper measures to guarantee safe transfer of very sensitive personal information. Had they done so, the file would never have found its way to the newspaper, exposing the man to the journalist and to his probing questions. Fortunately the newspaper agreed not to compound the problem by naming the man in its article.

The department apologized to the complainant. It also undertook to update its mailing lists, instruct employees on proper addressing and distribution of personal files and distribute information about the case to staff to illustrate the serious personal consequences of documents going astray. The complaint was well-founded.

Privacy not a screen for defaulting loans

Obviously not all complaints are well-founded. Privacy must sometimes give way before other demands—one of which is Canadians' obligations to pay their

debts. The Office continues to receive complaints that Human Resources Development Canada has "improperly disclosed" information about their defaulted Canada Student Loan payments to private collection agencies.

The government has a legitimate right and obligation to collect outstanding debts, and—having no collection agency of its own—it contracts debt collection to outside agencies. This does not violate the *Privacy Act*. Nevertheless, the Office ensures that contracts specify that agencies collection and use of the information does comply with the *Privacy Act*.

Surplus employee can see successful candidates' assessments

Government lay-offs prompted a complaint, not from one of the employees declared surplus, but from one offered a position. He complained that Public Works and Government Services had provided its personal assessment of his performance to an unsuccessful candidate to justify its decision to offer him, and not the other employee, the job.

In order to determine who would fill the remaining positions, Public Works developed selection criteria, established questions, a rating guide and the method of assessment for each job. From this process it established a list in reverse order of merit. Depending on the number of positions, employees were offered a position or declared surplus. Unsuccessful employees who grieved the process were provided the assessments of those ranked higher on the merit list.

This disclosure follows Public Service Commission policy which provides the information to ensure the fairness of the process; the employee can see that he/she was fairly evaluated against objective criteria and against other employees. The department collected the information to establish the reverse order of merit list. It is entitled to disclose the list and assessments to aggrieved employees to defend its decisions in establishing its merit list. In short, the disclosure is consistent with the purpose for the original collection. The Commissioner was satisfied that the disclosure of the higher-ranked employees' personal information was in accordance with the *Privacy Act*.

Must keep interview panel members' notes

Several RCMP members complained that they were unable to examine notes made by panel members during various selection boards. Members take handwritten notes to help them assess and rank the candidates. Some board members had kept the notes for as long as six months in their own files. Others' notes were shredded following the interviews, apparently on instructions from RCMP personnel staff. But ultimately all were destroyed—in two cases, between

the time the complainants sought access informally and then made formal requests.

The Act is clear; personal information used by a government institution to make an administrative decision about an individual is accessible and should be kept for a minimum of two years. Several board members interviewed could see no difficulty with retaining the notes. In fact, next year's non-commissioned officer selection boards will include a candidate de-briefing which is likely to require board members to retain their notes to go over individuals' answers to specific questions.

The RCMP has agreed to change its policy and will gather members' notes at the conclusion of the process and keep them in staffing files.

Garnishment notice not an "improper disclosure"

A Toronto woman argued that Revenue Canada's notice to her former employer that she owed back taxes was an improper disclosure of her personal information.

After several attempts to collect the arrears (which the woman was trying to reduce by periodic payments), Revenue Canada sent her a "pre-legal" letter demanding a response in 15 days. When the letter and phone call to her workplace produced no response, Revenue Canada issued a "Requirement to Pay" notice against the employer. In the meantime, the woman had left the job and says she wrote to Revenue Canada to advise them.

The investigator found no trace of a hard copy of the woman's letter or any entry in the taxation computer diary. Since Revenue Canada was attempting to collect taxes owing, did not know that she had left the job, and its authority is set out in the *Income Tax Act*, the Commissioner concluded that there had been no improper disclosure.

Labour market survey not compulsory

Statistics Canada's surveys always prompt telephone calls to the Commissioner. A Montreal woman complained that a Statistics Canada's labour market survey was an excessive collection of personal information that she was told she must provide. She also objected to the survey taker's demand for access to her future tax returns, as well as her telephone number or that of a family member or friend. The woman wanted the Office's help in refusing to answer Statistics Canada's questions.

It appeared that Statistics Canada had sent the woman a letter of introduction prior to taking the survey, explaining that the survey is voluntary. Unlike the Census, there are no legal obligations to respond to Statistics Canada surveys. An enthusiastic Statistics Canada staffer may have attempted to persuade the woman to participate and his or her persistence may have given the woman the impression she had to respond. However, the documents are clear.

Since the study is a six-year longitudinal survey, participants are followed up at regular intervals. Statistics Canada asks for an alternate telephone number; for example, of family members or friends, if it is unable to reach the person for an extended period.

The request for access to future tax returns was intended to help reduce the burden on respondents—much of the financial information needed for the survey duplicates details in individual tax returns. The question was apparently hypothetical—to assess respondents' willingness to approve such a disclosure. It was never made.

The Commissioner concluded that Statistics Canada had the authority to conduct the survey, had properly explained its purpose and made it clear that participation was voluntary. Statistics Canada undertook not to approach the woman again although there is nothing to prevent her name from appearing at random in future surveys.

MPs have no special access

An individual complained that someone at Citizenship and Immigration had improperly disclosed information about him to a member of Parliament. The investigation confirmed that an immigration officer wrote to the MP providing information about the complainant's immigration status in Canada and his criminal record.

While the *Privacy Act* allows departments to disclose personal information to MPs (with the individual's consent) for the member to help resolve the constituent's problem, MPs have no special access rights to other individuals' records. In this case, the MP was not helping the person concerned. In fact, he was acting on behalf of the complainant's estranged wife. The department did not have the complainant's consent to disclose his information to the MP, nor was there any reason to do so. The Privacy Commissioner concluded that Citizenship had made an improper disclosure.

Regrettably, once personal information has been disclosed, it cannot be retracted. There is no remedy that can undo the damage to the individual. However, the

department has assured the Commissioner that there will be no repeat of the incident. Citizenship officials agreed to develop and disseminate a policy to provide better direction to departmental officials responding to MPs' inquiries about its clients.

Supervisor leaves; computer transferred—with employee files

A Health Canada employee inherited a new computer from a departing supervisor and got more than simply more power. He found notes about another employee's performance on the hard drive and reported the discovery to a departmental official.

Health Canada erased the information, apologized and has issued a directive to all staff to check computer hard drives before re-assigning them to other staff.

Unfortunately, restoring the other employees privacy is impossible. The case is an object lesson for everyone who stores personal data on computers with little thought for the long-term consequences. Without help from their minders, these machines never forget.

DND public affairs staff reveal details to media

Government public affairs staff are often between the proverbial rock and hard place; criticized by the media for being secretive and, in this case, by family members for being too open.

A young soldier died in tragic circumstances and his parents pressed for the details. Unsatisfied with DND's explanations, they went to the media. DND public affairs staff responded to journalists' questions with details about the soldier's alcohol problems and DND's attempts to help him. In another interview, the public affairs officer also revealed that the soldier had not named his parents as next-of-kin to be called in an emergency.

Video recordings of television interviews established two of the disclosures. A print journalist learned some of the details from one of the television interviews, not public affairs staff as the family maintained.

Nevertheless, the Commissioner concluded that the disclosures were improper. DND will revise its policy and provide information sessions to guide public affairs officers when handling media demands for personal information.

Human error misdirects mail

Two instances of human error saw mail delivered to wrong addresses.

In the first case, a man's Change of Address card—the notice to the local Canada Post letter carrier to intercept and forward his mail—ended up being delivered to his former landlord. Canada Post apologized for what was an isolated incident.

The second case was potentially far more damaging; a letter from Revenue Canada's Audit Services to a taxpayer was enclosed in material being mailed to a third party. Fortunately the recipient returned the letter to Revenue Canada; it contained information about the woman's income tax returns.

Apparently Revenue Canada's Toronto East Tax Services Office provides mailing service to its Audit Services Branch. Mailing staff had gathered up the woman's letter inadvertently with other material. Revenue Canada apologized to the woman, has changed some mailing procedures and now conducts routine spot checks to try to prevent any recurrence.

Employee tax guidelines working

Last year we reported Revenue Canada's introduction of guidelines on using employees' tax files for supervision and performance assessment. This year an employee complained that Revenue Canada had breached those guidelines by using his tax files to make a case for firing him.

The investigator examined the employee's personnel files and found that the employee and manager had repeatedly discussed his behaviour, absences from his desk and frequent personal phone calls. Concerned about the employee's low productivity and on-the-job activities, the manager asked for an Internal Affairs audit.

The audit followed the trail left by the employee as he accessed key tax data available on Revenue Canada's computer system—selected tax items, not the complete return. The audit revealed that the employee had unauthorized access to his own tax data, as well as those of several family members and an acquaintance, none of which were needed for his job. It also revealed that despite having earned income, the employee had not filed a tax return for several years.

However, the audit did not intentionally target the employee's tax data—it simply followed the trail he left which included accessing his own file. There were no tax details in his personnel files. While Revenue Canada ultimately fired the employee, it was due to his work habits, lack of productivity and unauthorized access to his own and others' tax data. The department also asked him to file tax returns for the missing years.

The Commissioner concluded that the complaint was not well-founded. Had the manager made a deliberate decision to investigate an employee's income tax return, the guidelines require him to provide substantial justification and obtain the approval of the assistant deputy minister.

Inquiries

Many callers cannot be helped because the Commissioner has no jurisdiction over the private sector; banks, insurance companies or transportation companies.

Some callers were angry about Sprint Canada's request for customers' SIN. Others objected to Purolator Courier requiring all employees to be fingerprinted. And several calls from Air Canada employees wanted investigators to examine the airline's use of personnel files and its access to employees' e-Mail.

Despite having been Crown corporations, neither Air Canada or Via Rail (also the subject of several inquiries) have ever been covered by federal privacy legislation. Employees have no legal right to examine their personnel records unless privacy rights are negotiated in collective agreements.

OC Transpo

Several calls from OC Transpo employees also denied access to their files illustrate the unusual status of the Ottawa-Carlton area's public transit company. Its regular routes to Hull, Quebec, make it an "interprovincial" service and thus federally-regulated. However, it is not subject to federal privacy legislation, nor the Ontario privacy act which covers other Ontario transit authorities.

According to the Ontario Privacy Commissioner's office, OC Transpo tries to follow the Ontario legislation. The Ontario Privacy Commissioner has been able to gain access to employee files except those dealing with harassment or grievance cases. These OC Transpo officials refuse to open.

Old Age Security Card - SIN

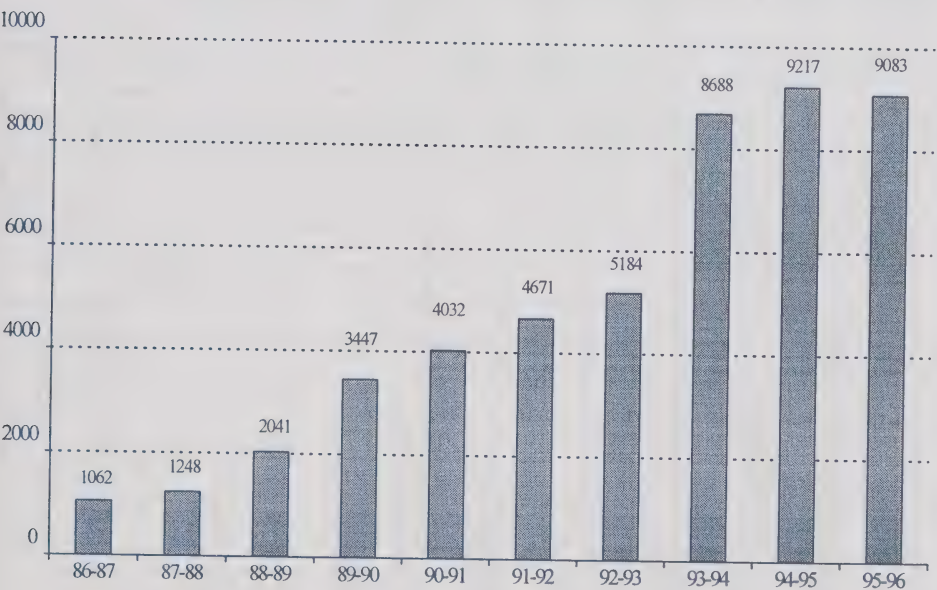
Three callers complained that their Social Insurance Number appears on their Old Age Security Cards, requiring them to reveal the SIN each time they use the card to identify themselves for benefits; for example, to get a seniors discount from a department store. Most of the callers declined to lodge a formal complaint, saying "it's not worth stirring up the hornet's nest". Clearly another senior disagreed because, shortly afterwards, the Office received a formal complaint which it is now investigating.

Personal Information Request Forms

Dozens of callers complain they are unable to find the Personal Information Request Forms needed to access their personal records. Several had been improperly directed to post offices; Canada Employment Centres don't have them, as advertised, and many tell us the Employment Centre staff have never heard of the forms. Since distribution of the supporting materials is Treasury Board's responsibility, staff attempt to point out the gaps to TB staff as they occur. In the meantime, however, the Office ships thousands of forms each year.

The forms and accompanying directory, *Info Source*, should be available in employment centres, federal government libraries and reading rooms, large public and university and college libraries, MPs' constituency offices and native band council offices.

Inquiries 1986-96



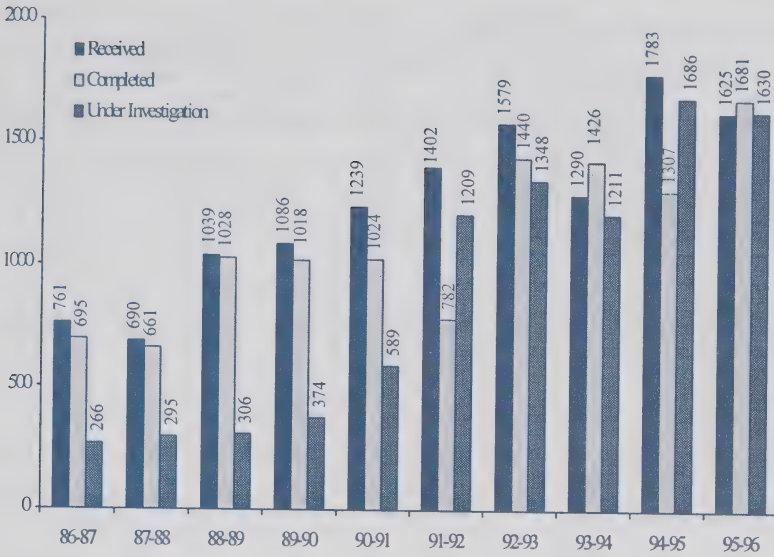
Top Ten Departments by Complaints Received

		Grounds			
Institution	TOTAL	Access	Time Limits	Privacy	
Correctional Service Canada	312	113	157	42	
National Defence	267	83	162	22	
Revenue Canada	235	58	141	36	
Royal Canadian Mounted Police	138	82	23	33	
Citizenship and Immigration Canada	106	31	67	8	
Canadian Security Intelligence Service	90	82	6	2	
Human Resources Development Canada	80	33	22	25	
Treasury Board of Canada Secretariat	67	3	0	64	
Canada Post Corporation	46	27	0	19	
National Archives of Canada	41	25	5	11	
OTHER	243	141	53	49	
	TOTAL	1,625	678	636	311

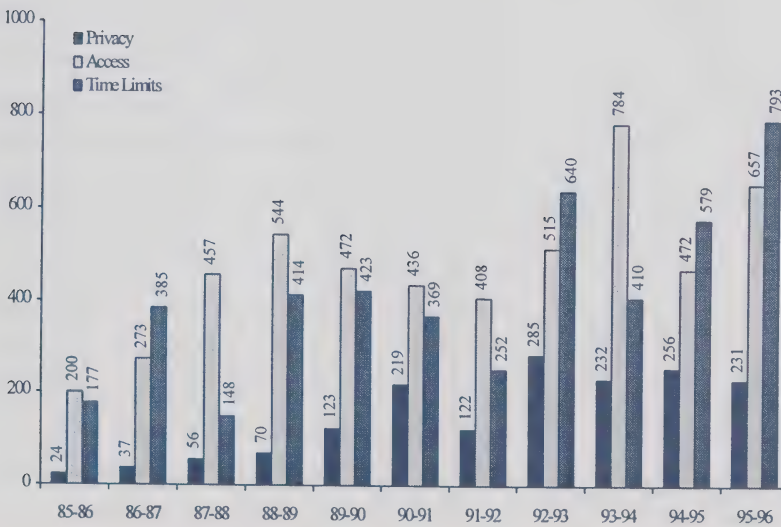
Completed Complaints by Grounds and Results

Grounds		Disposition					TOTAL
		Well-founded	Well-founded; Resolved	Not Well-founded	Resolved	Discon-tinued	
Access		12	126	470	21	28	657
	Access	12	119	430	19	26	606
	Correction/Notation	0	7	39	1	2	49
	Inappropriate Fees	0	0	1	1	0	2
	Index	0	0	0	0	0	0
	Language	0	0	0	0	0	0
Privacy		42	25	140	7	17	231
	Collection	2	0	36	1	2	41
	Retention & Disposal	10	6	9	2	2	29
	Use & Disclosure	30	19	95	4	13	161
Time Limits		584	3	154	0	52	793
	Correction/Time	2	0	2	0	1	5
	Time Limits	521	3	119	0	37	680
	Extension Notice	61	0	33	0	14	108
	TOTAL	638	154	764	28	97	1,681

Completed Complaints 1986-96



Completed Complaints and Grounds 1986-96



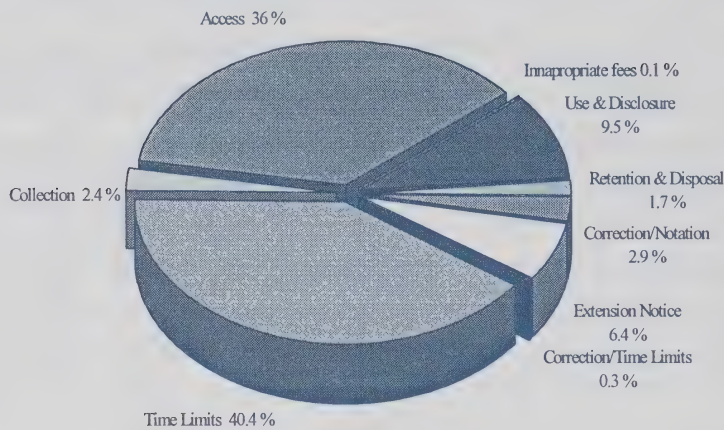
Completed Complaints by Department and Result

Department	Total	Well-founded	Well-founded; Resolved	Not well founded	Discontinued	Resolved
Agriculture and Agri-Food Canada	33	4	5	22	1	1
Atlantic Canada Opportunities Agency	1	1	0	0	0	0
Business Development Bank of Canada	1	0	1	0	0	0
Canada Council	1	1	0	0	0	0
Canada Mortgage and Housing Corporation	2	0	0	2	0	0
Canada Ports Corporation	2	0	1	1	0	0
Canada Post Corporation	41	10	10	18	1	2
Canadian Heritage	3	1	0	2	0	0
Canadian Human Rights Commission	4	0	0	3	0	1
Canadian International Dev. Agency	4	1	0	2	1	0
Canadian Security Intelligence Service	101	0	0	101	0	0
Citizenship and Immigration Canada	143	95	11	26	10	1
Commissioner of Official Languages	7	3	0	4	0	0
Consumer and Corporate Affairs	2	1	0	1	0	0
Correctional Investigator Canada	4	1	1	1	1	0
Correctional Service Canada	305	106	31	152	10	6
Elections Canada	1	0	0	1	0	0
Environment Canada	5	1	0	3	1	0
Farm Credit Corporation Canada	3	0	2	1	0	0
Fisheries and Oceans	4	1	0	3	0	0
Foreign Affairs and Int. Trade Canada	5	3	0	2	0	0
Freshwater Fish Marketing Corporation	2	0	0	2	0	0
Health Canada	22	4	5	10	0	3
Human Resources Development Canada	102	24	8	66	4	0
Immigration and Refugee Board	22	2	17	1	2	0
Indian and Northern Affairs Canada	1	0	1	0	0	0
Industry Canada	6	1	0	3	2	0
Inspector General of CSIS, Office of	1	0	0	1	0	0

Completed Complaints by Department and Result

Department	Total	Well-founded	Well-founded; Resolved	Not well founded	Discontinued	Resolved
International Centre for Human Rights	1	0	0	1	0	0
Justice Canada, Department of	19	2	2	15	0	0
Labour Canada	2	0	0	2	0	0
National Archives of Canada	32	5	3	23	1	0
National Arts Centre	1	0	1	0	0	0
National Capital Commission	1	0	0	1	0	0
National Defence	316	171	12	90	40	3
National Film Board	5	1	3	1	0	0
National Library	2	0	2	0	0	0
National Parole Board	17	1	4	12	0	0
National Research Council Canada	4	0	0	4	0	0
Natural Resources Canada	3	1	1	1	0	0
Office of the Auditor General of Canada	2	0	1	1	0	0
Privy Council Office	1	1	0	0	0	0
Public Service Commission of Canada	7	0	1	4	2	0
Public Works and Govt. Services Canada	21	1	7	9	1	3
Revenue Canada	253	171	10	66	5	1
Royal Canadian Mint	4	0	2	2	0	0
Royal Canadian Mounted Police	136	19	11	85	15	6
RCMP Public Complaints Commission	2	2	0	0	0	0
Social Sciences and Humanities Res. Coun.	1	0	0	1	0	0
Solicitor General Canada	3	0	0	3	0	0
Statistics Canada	1	0	0	1	0	0
Transport Canada	15	3	1	10	0	1
Treasury Board of Canada Secretariat	1	0	0	1	0	0
Veterans Affairs Canada	3	0	0	3	0	0
TOTAL	1,681	638	154	764	97	28

Complaints Completed by Grounds



Origin of Completed Complaints

Newfoundland	15
Prince Edward Island	14
Nova Scotia	50
New Brunswick	34
Quebec	172
National Capital Region Quebec	17
National Capital Region Ontario	349
Ontario	510
Manitoba	32
Saskatchewan	49
Alberta	132
British Columbia	293
Yukon	2
Outside Canada	12
TOTAL	1,681

Monitoring Compliance

The Branch's portfolio system had a thorough workout this year. Less time was spent on formal audits and follow-ups; far more on consultation and discussion with government staff. This reflects the evolving trends in the public service; becoming more active and service oriented.

Privacy staff are now more likely to be consulted early in program design and service delivery; in some cases, sitting on internal or interdepartmental committees to examine new initiatives. Two recent examples are the Office's work with Elections Canada on the permanent voters' register (see *A Vote for Privacy?* page 14) and ongoing discussions with the Justice Department on the new firearms registry. Preempting problems is the priority.

An ounce of prevention...

Ensuring compliance with the *Privacy Act* goes beyond auditing. Prevention also includes providing ongoing guidance to federal institutions. The timeliness of this guidance is crucial: the earlier the better. An increasing number of federal institutions recognize the benefits of involving portfolio leaders at the outset, whether developing new policy or launching activities which could affect clients' and employees' privacy. This year, staff dealt with many initiatives involving personal data; the following are some examples.

Atomic Energy Control Board: miner exposure to radon

Atomic Energy Control Board (AECB) sought the office's input when Dennison Mines asked AECB's consent to destroy files documenting workers' exposure to radon. Dennison had mined uranium in Elliot Lake during the 1950s and 1960s.

AECB regulates atomic energy in Canada. Among its responsibilities is monitoring the health effects of radioactive substances on workers. AECB requires uranium mining companies to keep records of workers' exposure to radon—a known carcinogen.

Rather than see destroyed an invaluable source of data for research into the long-term effects of radon exposure, AECB asked Dennison for the records. The company agreed. AECB was then faced with ensuring that its collection and use of this information complied with the *Privacy Act*.

AECB anticipates matching the data with Statistics Canada's mortality database to determine the effects of exposure on employees' lifespan and their mortality rates from lung cancer. The use is consistent with the mining companies'

original collection of the data — to monitor the health effects of exposure to radioactive substances.

To ensure that the database meets privacy requirements, the portfolio leader confirmed that:

- the research is part of AECB's responsibility—controlling health and safety aspects of radioactive substances;
- the information was originally collected directly from the individuals concerned (although AECB collected it second-hand from Dennison Mines). Obtaining consent of former employees for the transfer to AECB would have proven extremely difficult since virtually all left Elliot Lake when the mines closed;
- a retention schedule is in place. AECB intends keeping the information until the youngest miner has reached the age of 100 (assuming an age of 18 when hired);
- one current use of the data is consistent with the original collection: at the request of the Ontario Workers' Compensation Board, AECB confirms ex-miners' radon exposure to help the Board assess benefit entitlements for those diagnosed with lung cancer, and
- workers have right of access to their data. AECB will establish a personal information bank to hold the records. This prepares a safe repository for similar records should other uranium mining companies close operations.

Rideau Hall: Order of Canada nominees criminal record checks

Last spring, the Chancellery at Rideau Hall approached our office to discuss submitting Order of Canada nominees to criminal record checks. Finding a recipient had a criminal record could put the reputation of the Order at risk. Staff suggested a compromise which could satisfy the Chancellery's needs and respect the nominees' privacy. Nominees will be advised they have been recommended for the Order of Canada and asked to obtain confirmation from the RCMP that they have no criminal record or, if they prefer, to consent to the Chancellery verifying on their behalf. Nominees would then have the option to refuse, even if this meant withdrawing their names.

RCMP: removing personal data from surplus equipment

Following the revelation (in last year's annual report) that the Office had found RCMP documents in a safe it purchased from Crown Assets, the RCMP asked the portfolio leader to review a new section of its internal Security Manual

drafted to ensure that staff remove all information from surplus furniture before disposal.

Communications Research Centre: employee phone records

Telecommunications staff at the research centre (part of Industry Canada) asked for guidance on managers having access to employees telephone call records to contest long-distance charges or deal with suspected abuse of government long-distance lines. Privacy staff suggested advising employees before reviewing their call records and blocking out the last four digits of the number to protect the privacy of the party called. In fact, call records can be singularly unhelpful if employees deal regularly with the public from a central office which handles calls from across the country.

Public Works and Government Services: automating security screening

Screening potential government employees or contract staff for security and reliability is a huge job—PWGSC processes an estimated 29,000 a year. In an effort to simplify and automate the process, the department has developed the Personnel Screening Data Collection Automation System to reduce paperwork and turnaround time.

The new system uses software designed to help private companies working on government contracts to gather and transmit personal data on employees who need security screening. The employer can load the software into a personal computer, gather the information and send it on line to the department. PWGSC will offer the service to 2,600 companies which do business with the federal government, as well as government departments and agencies.

Given the amount and type of personal information required—family information and work history—the Office was concerned about making private sector organizations responsible for its collection and storage when they are subject to no privacy laws.

The department provided privacy staff with the proposed security agreement to bind companies which have delegated authority to collect and store the screening information. The agreements will impose contractual obligations to protect the information in accordance with the Government Security Policy and spell out the government's ownership of the information. A pilot project is underway to test the system.

Public Service Commission: privacy clauses for outside surveys

The Public Service Commission agreed to the portfolio leader's recommendations to change procedures following its disclosure to a survey firm of names, addresses and phone numbers of those using PSC recourse services. The company surveyed complainants to assess their satisfaction with PSC service. The most noteworthy change is the planned inclusion of clauses binding private companies to the provisions of the *Privacy Act*.

RCMP: suspends ride along program

Personal safety is a growing public concern. However, the RCMP agreed with the Office that exposing crime in a television program should not override the right of the individuals filmed during police patrols to be presumed innocent until tried in court. The RCMP interrupted its cooperation with the program *To Serve and Protect*, filmed in British Columbia, until producers agreed to blank out the faces, addresses and licence plates of the individuals—a common practice in similar U.S. programming. The RCMP undertook to develop a nation-wide policy on participating with communities and the media on fighting crime.

Human Resources: using Internet

The federal government too is on the Net. However, as governments go on-line, security of personal data is a pressing concern. Human Resources Development Canada (HRDC)—custodian of personal information on virtually every working Canadian—is the first to devise a federal policy on serving clients over the Net. HRDC sought the office's input to safeguard information collected from the general public visiting HRDC's Web site, and to prohibit transmission of personal information by Internet. HRD's policy should serve as a useful model for other government departments. (The Privacy Commissioner's own Web site is served by stand-alone terminals; there is no physical link to the internal network.)

Human Resources: the Electronic Labour Exchange

Another electronic project of HRDC is an Internet-based electronic labour exchange which "matches jobs to people and people to jobs". Employers use the exchange to specify the experience, skills and responsibilities of the position offered; job seekers describe their education, skills and experience. The exchange (an HRDC pilot project in the Ottawa area), attempts to bring the two together. Privacy staff offered HRDC guidance on collection and retention of job seekers' profiles, as well as subsequent uses of the personal data for labour market analysis.

Audits

The *Privacy Act* gives the Commissioner the power (and the discretion) to investigate federal government compliance with the act's fair information code—the rules governing collection, use, disclosure and disposal of individuals' personal information.

Traditionally, the Office selects a handful of organizations and examines their information handling practices (or, when the organization is large, one aspect of their operations). Given the near impossibility of systematic auditing, the Office has shifted its emphasis to examining privacy issues government-wide.

Nevertheless, the Office completed two audits during the past year—the Communications Security Establishment and the Canadian Centre for Management Development—and reviewed the internal compliance audit for a third—Canada Post's Central Division.

Communications Security Establishment (CSE)

CSE provides the federal government both the advice and the means to secure its own communications. It also provides the entire government with foreign "signals intelligence"; gathering and analyzing information about foreign countries by intercepting and studying their radio, radar and other electronic communications. CSE reports to the Minister of National Defence.

This audit proved to be one of the more complex the Office has undertaken, for several reasons. First, the nature of the material gathered and handled by CSE is extremely sensitive and demanded high-level security clearances for investigators, physical modifications to office space, and special equipment to process documents.

Second, in the midst of the audit, there were several public allegations that CSE was gathering data about Canadians and monitoring their legitimate political activities. Unfortunately, the ensuing public debate, and revelation that the office was conducting a routine audit, may have raised unrealistic expectations as to what the Privacy Commissioner could report.

Third, the *Official Secrets Act* also binds the Privacy Commissioner. This necessarily limits what he can report publicly.

Finally, and most germane to the Office's investigation, is that CSE's mandate is not set out in enabling legislation (as with most other government agencies)

except those unspecified powers conferred on the minister under the *National Defence Act*. Privacy audits usually rely on enabling legislation to assess an organization's compliance with the *Privacy Act*. A legislated mandate is the benchmark against which an organization's information management is measured; what information is collected and how, and how it is used, disclosed and ultimately destroyed. The government has given CSE a stated rather than legislated mandate to conduct foreign signals intelligence. It was against this stated mandate that the Office assessed compliance.

From a representative sampling of SIGINT data and reports, Office investigators concluded that CSE collects only information which serves the government's established foreign intelligence criteria. They found no evidence to support any allegations that CSE "targets Canadians" or monitors their communications. It is inevitable that any monitoring of foreign electronic communications will inadvertently trap information about some Canadians. However, CSE has strict procedures to minimize the possibility and to destroy any such information that does not meet government's foreign intelligence needs. Finally, the investigators also found that CSE's intelligence reports to government did not violate the act.

Nevertheless, the government should introduce legislation establishing explicitly a legal framework and review mechanism for CSE's operating programs and activities. Not only would this allow its personal information management practices to be measured objectively, it would establish in law protection for Canadians' liberties—as well as a clear underpinning for CSE. Legislation would stimulate informed debate about the agency's mandate and better understanding of its activities. In short, more light; less heat. The timing appears right: as we go to press, the government announced it will establish an independent oversight body for CSE.

Canadian Centre for Management Development (CCMD)

CCMD provides management orientation and training courses to senior federal government managers and appointees. Its two National Capital Region campuses and Edmonton satellite office employ about 200 government and private sector researchers, professors and other staff. The Centre holds personal information about both staff and approximately 30 per cent of the almost 12,000 students who attend CCMD courses and seminars each year. (No personal information is gathered from the other participants.)

This first audit of the CCMD examined how the Centre collects, keeps, uses, discloses, and protects its personal information holdings, and assessed employees' general knowledge and awareness of their obligations under the *Privacy Act*.

The audit identified several problems with the Centre's management of personal information. For example, files containing personal information were stored in insecure locations; some personal information holdings had not been identified and described in *Info Source*; disposal schedules had not been developed, or were not being applied, leading to information being stored longer than needed, and contracts requiring access to personal information did not bind contractors to comply with the *Privacy Act*. Before the audit, staff knew little about the requirements of the Act. This explains most of the shortcomings identified. However, staff understood the concept of "confidentiality" well, and were willing to learn.

Privacy audit staff made several recommendations to the Centre, including:

- within one year, implement a personal information management policy covering the entire cycle from collection to disposal;
- properly organize, file and control circulation of its personal information holdings;
- revise its forms to avoid collecting unnecessary personal details from students and to advise them of their rights under the *Privacy Act*;
- with the help of the National Archives, implement a retention and disposal schedule for its personal information holdings, and review its current holdings to determine those which should be disposed of;
- implement measures to protect its personal information holdings from unauthorized access;
- exercise caution when transmitting personal information by fax;
- state in all contracts with third parties that the personal information to which they have access is under the control of the CCMD and subject to the Act;
- educate current and new CCMD employees on these initiatives and about the requirements of the Act; and
- accurately describe all of its information holdings in *Info Source*.

CCMD reacted quickly to the recommendations and is taking action to deal with all issues raised.

Canada Post Corporation - Huron Division

Advised of the Office's planned audit, Canada Post reacted by launching its own. Spurred by discussion in the Privacy Commissioner's last annual report about

Huron Division managers keeping "shadow" files on their employees (and refusing access to the files under the *Privacy Act*), Canada Post's Central Area privacy office began examining former Huron Division files.

The audit confirmed the problem of "shadow" files and led Canada Post to concrete action. Managers were told that they "may" retain in their personal files documents such as attendance calendars or other records needed to "support the supervision of employees, especially at remote work sites". However, two conditions were imposed:

- these documents must only be copies of documents found in official employee files, and
- the documents must be described in a new personal information bank listed in *Info Source*.

Privacy staff examined the results of Canada Post's preliminary compliance review and concluded that the proposed changes to the corporations's business practices made it unnecessary for the Office to conduct its own audit at this point. Instead the Office will monitor complaints against Canada Post to help assess whether the corrective action produces a long-term solution.

Citizenship & Immigration (CIC)

Last year we reported recommendations from our audit of CIC's informatics system. CIC was (and still is) in the midst of a massive re-organization. Despite these pressures, CIC has prepared an action plan for each of the recommendations. It has also agreed to present specific compliance reports and action plans to respond to the Office's requests prompted by the audit. These include:

- developing a department-wide plan for ongoing privacy training;
- completely overhauling its listings in *Info Source*;
- reviewing a sample of its information sharing agreements;
- reviewing its retention and disposal schedules for personal records, and
- reviewing its personal information collection and procedures to ensure compliance with the *Privacy Act*.

Follow-ups

This year, staff continued following up earlier audits to determine whether federal institutions complied with our recommendations. Once again, staff found a high degree of compliance.

Canadian Human Rights Commission (CHRC) Staff returned to the Commission, first audited in 1992. CHRC has begun addressing several problems the audit identified, including how the Commission describes, keeps and protects access to its paper and electronic files. CHRC has also developed guidelines for its staff on using fax machines to transmit sensitive complaint information.

Some work remains to be done on three recommendations. The Commission has not conducted a complete security and risk assessment for areas where complaints are processed and stored. And while CHRC contracts now require outside contractors to respect the confidentiality of the information they process on its behalf, they do not contain satisfactory clauses clearly establishing that any personal information gathered is deemed to be under the control of the Commission and subject to the *Privacy Act*. Finally, the Commission's mailing lists need to be described in *Info Source* as a personal information bank, rather than a general information holding.

National Research Council (NRC) Following the Office's 1992 audit, NRC has complied with all but one recommendation, and work on the one outstanding issue—weeding out old personal records—is well under way.

NRC has

- written explicit privacy language into its contracts with contractors providing Employee Assistance Plan services;
- listed in *Info Source* its collection of personal information on employees who have undergone reliability checks;
- split its personnel files into three components to control access to the information, and destroyed duplicate dormant files maintained in a regional office, and
- designed a segment for an existing course, *Managing a Diverse Workforce*, given nationally to improve employees' awareness of privacy law. The course is mandatory for managers, supervisors and all headquarters staff.

National Defence (DND) DND has acted on all but three of the outstanding recommendations from the Office's 1991 audit. Those three concerned Canadian Forces Base Lahr, now closed.

Royal Canadian Mounted Police (RCMP) All eight outstanding recommendations from the 1991 audit have been dealt with. They included creating a new information bank for Benefit Trust Fund records, amending other

bank descriptions, extending the retention period for some records to the required two years, and ensuring that crime victims consent before investigators give their names to victim's services volunteers.

Information Sharing Study

Background This year the branch analysed returns from its survey of government sharing and data matching of personal record holdings. The survey attempted to identify both disclosures under various information sharing agreements and "arrangements", and data matches—of which the Commissioner receives suspiciously few notifications.

Statistics Canada staff advised on the structure of the questionnaire and an advisory committee guided the project and reviewed the findings. The Office distributed the survey to all deputy heads in February 1995 and completed data collection late in 1995. The final results are based on 107 of 109 institutions responding. Some blatant errors were corrected but generally the data was entered as reported. While the survey results are not exhaustive (and have not been verified), they are revealing.

Why sharing needs tallying Although the *Privacy Act* protects clients' and employees' personal information, the law allows several disclosures. One of these permits federal government agencies to share information under "an agreement or arrangement" with other levels of government and international organizations. However, the sharing is to be described publicly so that individuals understand how government uses and discloses their information. This is the "informed" part of informed consent.

The Act is also clear that personal information collected for one purpose cannot be used for other unrelated purposes—this includes sharing between programs within a single department for which there is no provision. New uses for data are permitted if they are "consistent" with the original purpose, the Commissioner is notified and the new use described in *Info Source*.

The findings The results are summarized here. Datamatches were examined to determine whether they started before the Treasury Board's policy was put in place or, if after, whether the Commissioner was notified as required.

Category	Number	%
Institutions surveyed	109	100
Institutions responding	107	98
Institutions sharing internally	35	33
Number of internal sharing arrangements	137	N/A
Number reported in <i>Info Source</i>	70	51
Institutions sharing externally	51	48
Number of external arrangements/agreements	861	N/A
Number reported in <i>Info Source</i>	591	69
Data matches	15	14
Number reported in survey	66	N/A
Data matches reported in	6	9

Internal Sharing Few *Info Source* bank descriptions mention internal sharing clearly and explicitly. There are some oblique references to the program with which the information is shared, other examples require the reader to refer back to program records. There is often no apparent consistency between the new and original collection purpose. Finally, information from several programs is stored in an integrated computer system, providing staff access to (and, presumably, use of) all information in the system.

Even those 70 cases of sharing which departments consider they have reported in *Info Source* are difficult to detect by experienced staff, let alone the public. They demand both careful perusal and liberal interpretation.

External Sharing External sharing is reported more frequently in *Info Source*, occasionally (but not usually) citing a clear authority for the sharing—one listing

named "the Constitution of Canada" as the authority. No further details were provided.

The number of sharing agreements and arrangements may appear high. However, they are inflated by two departments, Statistics Canada and Revenue Canada which together reported 434—more than 50 per cent of the total 861. Of this 434, 319 were covered by written agreements.

Datamatching The survey reports 66 data matches; *Info Source* only six. Our already low expectations were based on the 30 proposals submitted for the Commissioner's review since 1987. Departments have apparently lost track of even these 30 and public descriptions of the six are unclear. One institution's survey response maintained that it did not data match yet all its personal information bank descriptions state that the information may be used for datamatching.

There was another anomaly: some matches were reported by one institution, but not the other. Although the reporting institution may be considered the "matching" institution (and the other merely provided information), at the least the information provider should report the disclosure as external sharing. This was not the case.

Only eight internal data matches were reported; surprising given the proliferation of computer systems.

While Treasury Board's instructions on conducting a data match are clear, some privacy coordinators seem unsure about its application. The result: neither the public or the Commissioner is being told. Far greater cooperation is needed between departmental privacy coordinators and the program staff who devise the matching proposals.

Conclusions It is evident that the returned questionnaires are not always accurate or complete; for example, they revealed:

- incomplete responses to questions on the existence of written agreements to cover an activity;
- no list of personal information banks which describe a sharing or matching activity;
- information the Office knows to be inaccurate;
- failure to list data matches reviewed by the Office, and
- suspected under-reporting of both matching and sharing.

While it may be risky to draw conclusions from the returns, one thing is clear—*Info Source* is a difficult tool to use in its present form, even for experienced staff. It demands careful perusal to determine the extent of government datamatching, or consistent uses departments make of personal information under its control. Even then, the references are often oblique.

Our sympathy is with uninitiated readers trying to find their way through this thicket. It's time for the government to be much clearer and more forthright on its uses of clients' and employees' data.

In the Courts

Minister of Finance v. Michael Dagg

The Supreme Court of Canada has agreed to hear Mr. Dagg's appeal of a lower court decision denying him access to the Department of Finance's after-hour employee sign-in sheets. The Privacy Commissioner will intervene in the case.

Last year's annual report described the Federal Court of Appeal's decision (see page 26) which established clearly that the *Privacy Act* and the *Access to Information Act* are of equal status. Once information sought under the Access Act is found to be "personal", it may only be given to third parties if disclosure is permitted by the *Privacy Act*.

The Court has yet to set a date for the hearing.

Rubin v. Clerk of the Privy Council

This case, although brought under the *Access to Information Act*, also has significance for the Privacy Commissioner because an identical provision appears in section 33(2) of the *Privacy Act*.

The Supreme Court confirmed a lower court decision that no-one has a right to have access to another person's representations to the Information Commissioner and that confidentiality continues, even when the investigation is completed. Mr. Rubin had argued that the confidentiality of representations should end, once the investigation is finished.

The ruling suggests that the Court would reach a similar conclusion about representations to the Privacy Commissioner.

Privacy Commissioner v. Canada Labour Relations Board

The Federal Court heard this case early in June. The case, reported in some detail in the 1994-95 report (see page 27) concerns access to personal information contained in handwritten notes taken by Board members at a labour relations hearing. The decision is expected in the Fall.

Taking the Show on the Road

Despite government's apparently firm conviction that the Privacy Commissioner has no education role (and certainly needs no money to inform Canadians) taxpayers think otherwise. The Office handled 1304 publication and media requests and there were more than 30,000 visits to the Commissioner's new Web site. In fact, the Office was one of the first dozen federal agencies to establish a site as part of the Open Government pilot project. In addition to providing the Office's information and publications, the site links to other privacy sites.

Commissioner and staff gave more than 30 speeches this year—and had to gracefully decline almost as many. The cupboard is bare.

Consumers, business, professionals and the media are alive to privacy as an issue. The recent survey by Ekos Research Associates for the Public Interest Advocacy Centre (PIAC) and the Fédération nationale des associations de consommateurs du Québec (FNACQ) demonstrates the public's growing concern.

Overwhelmingly Canadians want to be informed about the collection of their personal information and the uses to which it is put. They insist that their permission be obtained before their information is passed to another organization. And 87 per cent think government should treat the issue as a priority. (Copies of the entire report are available from PIAC in Ottawa and FNACQ in Montreal.)

Among the speaking engagements, Commissioner and staff spoke about the privacy implication of information technology to

- the Canadian Telecommunications Superconference;
- the 11th annual General Assembly of the World Teleport Association;
- the annual Winter Cities conference of northern mayors;
- the Communications Security Establishment's annual computer Security Conference, and
- the University of Victoria's Leading Edge Technologies conference.

Interest in bringing the law into the information age led to speeches to the Canadian Bar Association and the Commissioner delivering

- the Law Society of Manitoba's annual Isaac Pitblado lecture;

- the annual I.P Sharp lecture to the University of Toronto's Information Management faculty, and
- a Legislative Library Noon-Hour talk to New Brunswick legislators, staff and the public.

Where to draw the line on DNA testing—in criminal investigations and insurance underwriting—were the subject of speeches to

- the *Genetics and the Law* symposium at Osgoode Hall, Toronto, and
- the annual conference of the Canadian Life Insurance Medical Officers' Association in Regina.

Corporate Management

The Privacy and Information Commissioners share premises and administrative services but operate independently under their separate statutory authorities. Corporate Management Branch provides centralized administrative services to avoid duplication of effort and realize cost savings to the government. The services include finance, personnel, information technology advice and support, telecommunications, library services and general administration.

The Branch has just 15 staff (who perform a variety of tasks) and a budget representing 15 per cent of the overall OIPC budget. Subject to modest savings through information technology, the Branch has gone as far as it reasonably can to simplify and streamline service delivery.

Resource Information

The Offices' combined Main Estimates for the 1995-96 fiscal year were \$6,186,000, a decrease of \$236,000 over 1994-95. Actual expenditures for the 1995-96 period were \$6,516,792 of which, personnel costs of \$5,435,439 and professional and special services expenditures of \$565,170 accounted for more than 92 per cent of all expenditures. The remaining \$516,183 covered all other expenditures including postage, telephone, office equipment and supplies.

Figure 1: 1995-96 Resources by Organization/Activity

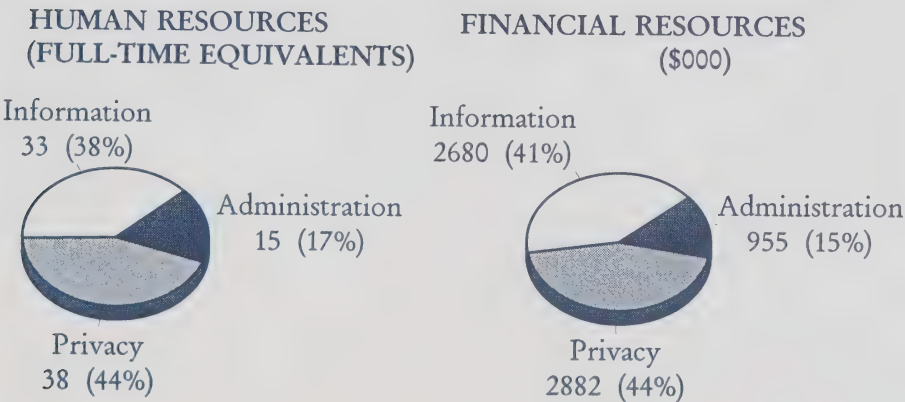
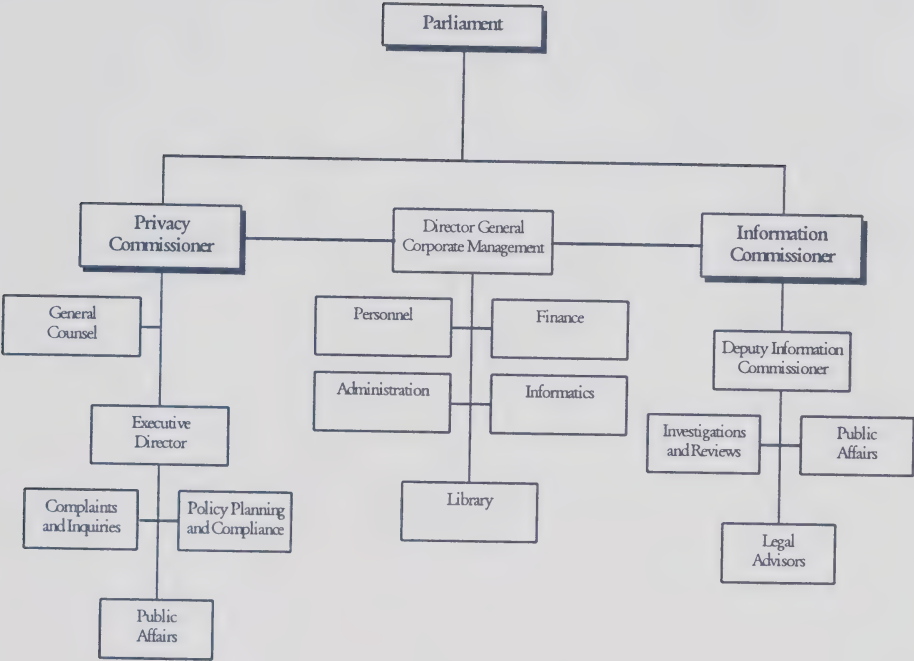


Figure 2: Details by Object of Expenditure

	Information	Privacy	Corporate Management	Total
Salaries	1,938,644	2,252,614	585,181	4,776,439
Employee Benefit Plan Contributions	262,400	307,570	89,030	659,000
Transportation and Communication	56,724	72,323	92,391	221,438
Information	27,046	46,635	5,376	79,057
Professional and Special Services	302,101	168,871	94,198	565,170
Rentals	2,352	589	13,766	16,707
Purchased Repair and Maintenance	4,695	143	8,957	13,795
Utilities, Materials And Supplies	24,350	12,864	37,752	74,966
Acquisition of Machinery and Equipment	61,328	19,375	28,429	109,132
Other Payments	576	512	-	1,088
Total	2,680,216	2,881,496	955,080	6,516,792

* Expenditure Figures do not incorporate final year-end adjustments reflected in the Offices' 1995-96 Public Accounts.

Organization Chart



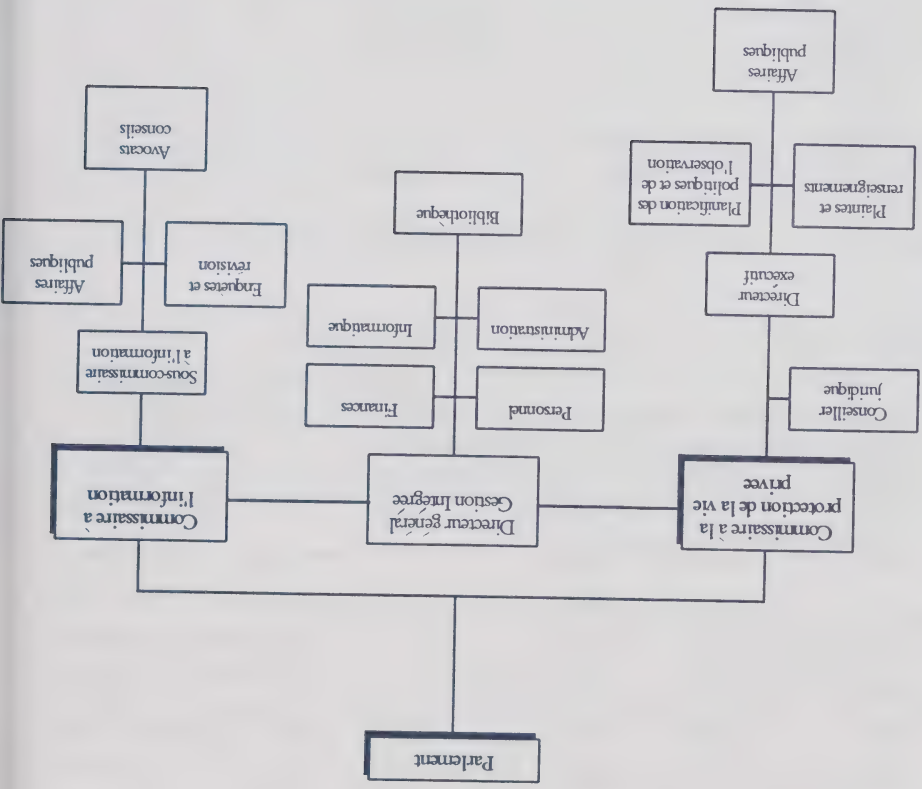


Tableau 2: Ventilation par type de dépense

	Information	Vie privée	Gestion intégrée	Total
Salaires	1,938,644	2,252,614	585,181	4,776,439
Contributions aux régimes d'avantages sociaux	262,400	307,570	89,030	659,000
Transports et communications	56,724	72,323	92,391	221,438
Information	27,046	46,635	5,376	79,057
Services professionnels et spéciaux	302,101	168,871	94,198	565,170
Locations	2,352	589	13,766	16,707
Achat de services et réparations	4,695	143	8,957	13,795
Services publics, fournitures	24,350	12,864	37,752	74,966
Achat de machines et d'équipement	61,328	19,375	28,429	109,132
Autres dépenses	576	512	-	1,088
Total	2,680,216	2,881,496	955,080	6,516,792

• ces dépenses ne relient pas les rajustements de fin d'exercice indiqués aux Comptes publics des Commissariats pour 1995-96

Direction de la gestion intégrée

Par souci d'économies et d'efficacité, le Commissariat à la protection de la vie privée et le Commissariat à l'information partagent leurs locaux et leurs services administratifs. Les deux commissariats fonctionnent cependant de façon indépendante en vertu des deux lois habilitant leurs opérations. Les services administratifs sont assurés par la Direction de la gestion intégrée, et comprennent les finances, le personnel, les conseils et le soutien informatique, les télécommunications, la bibliothèque et l'administration générale.

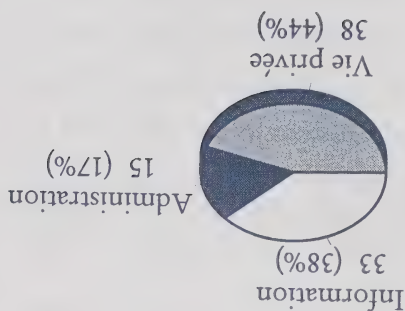
Les salaires des 15 employés polyvalents de la Direction représentent 15 pour cent du budget total des deux commissariats. De modestes économies réalisées dans le domaine de l'informatique ont permis à la Direction de simplifier et d'alléger la prestation de ses services au mieux de ses possibilités.

Description des ressources

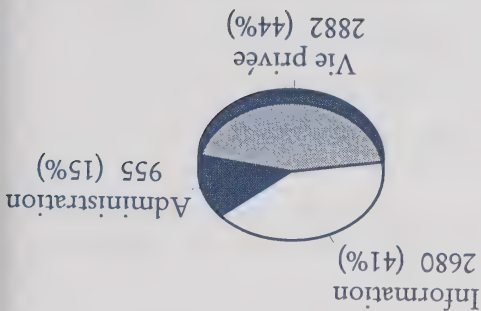
Le budget combiné que les deux Commissariats avaient projeté pour l'exercice financier 1995-96 s'élevait à 6 186 000 \$, en baisse de 236 000 \$ par rapport à l'exercice précédent. Les dépenses réelles pour l'exercice 1995-96 étaient de 6 516 792 \$, dont 92 pour cent ont été consacrés aux salaires (5 435 439 \$) et aux services professionnels et spéciaux (565 170 \$). Le solde de 516 183 \$ a permis de défrayer les coûts de la poste, du téléphone, des fournitures et du matériel de bureau.

Tableau 1 : Ventilation par organisme/activité

RESSOURCES HUMAINES (ÉQUIVALENTS TEMPS PLEIN)



RESSOURCES FINANCIÈRES (\$000)



- la Conférence de l'Université de Victoria sur les technologies de pointe.
- La mise en oeuvre d'une protection juridique de la vie privée nous a mené devant les membres de l'Association du Barreau canadien, et le Commissaire a prononcé l'allocation annuelle Isaac Pitblado du Barreau manitobain;
- l'allocation annuelle I.P. Sharp de la faculté de gestion de l'information de l'Université de Toronto; et
- un discours auprès du public, des députés néo-brunswickois et de leur personnel dans le cadre des Rencontres du midi organisées par la Bibliothèque du parlement provincial.
- Les limites au dépistage génétique (dans le cadre d'enquêtes criminelles ou d'assurance-vie) ont souligné notre participation :
- au symposium organisé au *Osgoode Hall* de Toronto sur la génétique et la loi; et
- à la Conférence annuelle de l'Association canadienne des directeurs médicaux en assurance-vie.

Le rôle de missionnaire des Affaires publiques

Le gouvernement semble croire qu'il ne revient pas au Commissaire à la vie privée d'informer ni d'éduquer les Canadiens (et que le Commissaire n'a donc nul besoin d'argent à cet effet...). Les contribuables ne partagent heureusement pas cette opinion. En effet, nous avons répondu cette année à près de 1304 demandes de publications, et plus de 30,000 personnes ont consulté notre nouveau site Web. Nous étions d'ailleurs parmi les premiers organismes fédéraux à établir un tel site dans le cadre d'un projet pilote visant à faciliter l'accès de la population aux renseignements gouvernementaux. Notre site permet d'accéder aux renseignements et aux documents que nous fournissons à la population, ainsi qu'à d'autres sites reliés à la protection de la vie privée.

À la trentaine de discours prononcés tant par le Commissaire que par son personnel se rajoute un nombre sensiblement équivalent de demandes que nous avons malheureusement dû refuser, faute de ressources.

La protection de la vie privée préoccupe autant le consommateur que l'entreprise privée, le professionnel que le journaliste. Et la preuve s'en trouve dans le sondage qu'effectuait récemment la maison Ekos Research pour le compte du Centre pour la défense de l'intérêt public (CDIP) et la Fédération nationale des associations de consommateurs du Québec (FNACQ).

Les Canadiens veulent d'abord et avant tout connaître les détails entourant la collecte de leurs renseignements personnels et l'usage qui en est fait. Ils tiennent absolument à approuver ou non la transmission de ces renseignements à un autre organisme. Et 87 pour cent d'entre eux croient que le gouvernement devrait s'attaquer au plus tôt à cette question. (Pour des copies du rapport intégral, veuillez vous adresser au CDIP à Ottawa ou à la FNACQ à Montréal.)

Les principaux discours portant sur les impacts de la technologie de l'information sur notre vie privée ont vu le Commissaire et son personnel s'adresser aux participants de

- la Superconférence canadienne sur les télécommunications;
- la 11^e Assemblée générale annuelle de la *World Teleport Association*;
- l'Assemblée annuelle des maires des Villes d'hiver nordiques;
- la Conférence annuelle sur la sécurité informatique, organisée par le Centre de sécurité des télécommunications; et

La Cour suprême du Canada a accepté d'entendre l'appel interjeté par M. Dagg du jugement de la Cour d'appel du Canada, dans lequel cette dernière lui avait interdit l'accès aux fiches d'entrée que doivent remplir les employés du ministère des Finances travaillant en dehors des heures ouvrables. Le Commissaire à la vie privée participera à la cause.

Notre rapport annuel de l'an dernier résumait (en page 29) le jugement de la Cour d'appel, laquelle avait clairement statué sur l'égalité de la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels* : tout renseignement demandé en vertu de la première loi, mais jugé de nature "personnelle", ne peut être divulgué à des tiers que si la seconde loi le permet. Une date reste à être fixée pour cette cause.

Rubin c. le greffier du Conseil privé

Le Commissaire à la vie privée s'est intéressé à cette cause, bien qu'elle ait été entendue en vertu de la *Loi sur l'accès à l'information*, car elle portait sur une disposition de cette dernière se retrouvant également à l'article 33(2) de la *Loi sur la protection des renseignements personnels*.

La Cour suprême avait confirmé que personne ne pouvait recevoir la communication des observations présentées au Commissaire à l'information par des tiers lors des enquêtes de ce dernier et même après la fin de celles-ci. Le libellé du jugement porte à croire que la Cour aboutirait aux mêmes conclusions quant aux observations présentées au Commissaire à la vie privée.

Commissaire à la vie privée c. le Conseil canadien des relations de travail

Cette cause devrait être entendue au début du mois de juin. Notre rapport annuel de 1994-95 (en page 30) présentait les détails de cette cause traitant de l'accès aux renseignements personnels contenus dans les notes manuscrites prises par les membres du Conseil lors des audiences. Le tribunal devrait statuer sur ce cas cet automne.

Conclusions Les réponses que nous avons reçues des organismes ne sont évidemment pas toujours exactes ni complètes. À preuve :

- des réponses incomplètes aux questions liées à l'existence d'accords écrits découlant d'un programme;
- aucune liste de ceux des fichiers de renseignements personnels visés par un partage ou un couplage de renseignements;
- des renseignements dont le Commissariat sait pertinemment qu'ils sont inexact;
- l'oubli d'inscrire dans les réponses les couplages de renseignements étudiés par le Commissariat; ou encore
- la perception que tant le partage que les couplages de renseignements n'ont pas tous été rapportés lors du sondage.

Il semble risqué de tirer des conclusions de réponses apparemment incomplètes. Mais il est clair que le répertoire *InfoSource* est dans sa forme actuelle un outil trop compliqué à utiliser, et ce même pour les gens qui en ont l'habitude : il faut le lire avec beaucoup de soin avant de pouvoir saisir le nombre et l'étendue des couplages de renseignements qu'effectue le gouvernement fédéral, ou même ce que ce dernier considère être des utilisations compatibles de ceux de nos renseignements sous son contrôle.

Nous vous plaignons, vous, lecteurs non initiés! Il est temps que le gouvernement fédéral nous informe davantage et mieux de toutes les utilisations qu'il fait des renseignements personnels qu'il détient à notre sujet et sur ses employés.

Partage externe de renseignements *InfoSource* s'en tire mieux à ce chapitre, les descriptions du partage externe de renseignements y étant plus fréquentes. Mais si certaines comportent une justification juridique sans équivoque, beaucoup ne le font pas : une des descriptions invoquait par exemple la *Constitution* comme texte justificatif, sans plus de détails!

Le nombre des accords et ententes de partage externe de renseignements peut sembler élevé. Mais sur un total de 861 ministères, plus de la moitié (434) proviennent de deux ministères (Statistique Canada et Revenu Canada) et de ce nombre 319 font l'objet d'un accord écrit.

Couplages de renseignements Notre sondage a trouvé 66 couplages de données alors qu'on n'en retrouve que six dans *InfoSource*, soit bien moins que nous ne l'aurions cru : nos attentes, pourtant faibles, reposaient sur les quelque 30 avis de couplage envoyés depuis 1987 au Commissaire pour son approbation. Il semble que les organismes fédéraux en ont perdu la trace, et les six qui restent ne sont même pas clairs. Un organisme nous a même répondu ne pas effectuer de couplage de données, et ce en dépit des descriptions publiées dans *InfoSource* et stipulant que les renseignements de l'organisme pouvaient faire l'objet de couplages.

Autre anomalie : lors d'un couplage impliquant deux organismes, l'un répondait participer au couplage, mais pas l'autre. Certains pourront dire que le second organisme était dans le vrai, puisqu'il n'était que le fournisseur des renseignements couplés par le premier. Ce second organisme aurait cependant dû à tout le moins rapporter ce partage externe de renseignements, ce qu'il n'a pas fait.

Compte tenu de la prolifération des réseaux informatiques au sein du gouvernement fédéral, nous avons également été surpris de ce que seulement huit couplages internes de renseignements nous aient été rapportés.

Les obligations que doit respecter un organisme fédéral avant d'entreprendre un couplage de renseignements sont clairement stipulées dans le *Manuel* du Conseil du Trésor sur la protection des renseignements personnels. Mais les coordonnateurs à la vie privée de certains ministères ne comprennent pas bien ces obligations. De plus, ces coordonnateurs ne peuvent pas s'y conformer tant qu'ils ignorent si leur organisme souhaite effectivement entreprendre un couplage de renseignements. Et puisque les organismes ne contrôlent pas leurs utilisations de renseignements personnels, ils ne peuvent pas identifier le début d'un couplage de renseignements n'ayant pas été autorisé par le Commissaire à la vie privée.

Résultats Les documents découlant du sondage comprennent divers tableaux analytiques. Les données suivantes n'en représentent que les faits saillants.

Catégorie	Nombre	%
Organismes visés par le sondage	109	100
Organismes ayant répondu au sondage	107	98
Organismes partageant des renseignements à l'interne	35	33
Ententes de partage interne de renseignements	137	s/o
Ententes internes décrites dans <i>InfoSource</i>	70	51
Organismes partageant des renseignements à l'externe	51	48
Ententes/accords de partage externe de renseignements	861	s/o
Ententes/accords externes décrits dans <i>InfoSource</i>	591	69
Organismes couplant des renseignements	15	14
Couplages de renseignements	66	s/o
Couplages de renseignements décrits dans <i>InfoSource</i>	6	9

Partage interne de renseignements Notre révision des ententes de partage interne de renseignements inscrites au répertoire *InfoSource* révèle que ce dernier reste généralement vague et peu explicite à ce sujet. Certaines descriptions font d'obscures références aux activités menant au partage interne, alors que d'autres obligent le lecteur à fouiller les explications des divers types de renseignements détenus par les organismes. Les fins premières avouées de collecte et les fins dites connexes semblent rarement compatibles, et les renseignements découlant de diverses activités sont souvent entreposés au sein du même système informatique, de ce fait accessibles (et probablement utilisés) par de nombreux employés.

Si notre personnel, pourant expérimenté, a eu de la difficulté à découvrir dans *InfoSource* la description des 70 ententes de partage interne de renseignements qu'a révélés le sondage, qu'en est-il du public? La lecture de ce répertoire exige-t-elle une attention qu'une bonne dose d'interprétation.

soient pas approfondis, ils n'en sont pas moins révélateurs et reposent sur 107 des 109 organismes participants.

Pourquoi dénombrer ces accords ou ententes La Loi sur la protection des renseignements personnels protège bien les renseignements personnels que détient le gouvernement fédéral au sujet de ses clients et de ses employés, mais elle en autorise aussi la communication dans plusieurs cas. Ainsi, un organisme fédéral peut communiquer des renseignements en vertu d'un accord ou d'une entente liant d'autres paliers de gouvernement ou un organisme étranger. Ce partage doit cependant être décrit publiquement afin que la population puisse comprendre comment le gouvernement fédéral utilise et communique les renseignements qui la concernent. Cette information permet un consentement éclairé de la part de la population.

La Loi stipule également clairement qu'un renseignement recueilli à une certaine fin ne peut pas servir à d'autres fins, dont le partage de ce renseignement au sein même de l'organisme l'ayant recueilli. La Loi ne permet pas ce type de communication. Il est cependant possible de se servir d'un renseignement à une fin "compatible" avec l'objectif initial de la collecte si le Commissaire à la vie privée en est prévenu et si la nouvelle utilisation est décrite dans *InfoSource*.

- inscrit au répertoire *InfoSource* sa collecte de renseignements dans le cadre de vérifications de fiabilité;
 - scinde ses dossiers d'employés en trois composantes distinctes afin d'y réduire l'accès, et détruit les duplicatas de dossiers provenant d'un bureau régional; et
 - incorporé à un de ses cours d'orientation une formation reliée aux lois protégeant la vie privée. Ce cours est obligatoire pour les gestionnaires, surveillants et tout le personnel du siège social.
- Défense nationale** Les trois seules recommandations que le ministre n'avait pas encore appliquées suite à la vérification que nous y avons effectuée en 1991 n'ont plus raison d'être, puisqu'elles visaient la base militaire de Lahar, qui a depuis été fermée.

Gendarmerie royale du Canada Les huit recommandations que la GRC devait encore appliquer suite à notre vérification de 1991 l'ont été. Ces recommandations visaient l'inscription au répertoire *InfoSource* d'un nouveau fichier de renseignements reliés à la Caisse fiduciaire de bienfaisance, la correction du libellé d'autres fichiers, la prolongation de la durée de conservation de certains dossiers jusqu'aux deux ans stipulés dans la *Loi sur la protection des renseignements personnels*, ainsi que la nécessité d'obtenir le consentement des victimes de crimes avant que les enquêteurs ne communiquent leurs coordonnées à des groupes d'entraide spécialisés.

Étude sur le partage de renseignements

Rappel Cette année, la direction s'est penchée sur les réponses qu'elle avait reçues l'an dernier au sondage qu'elle effectuait sur le couplage et le partage de renseignements personnels au sein du gouvernement fédéral. Ce sondage résultait des continues découvertes de nouveaux accords ou de nouvelles "ententes" que soulevaient les vérifications et les enquêtes du Commissariat.

Statistique Canada nous a offert ses conseils quant à notre questionnaire, et l'ensemble du projet a été piloté par un comité consultatif, lequel a également révisé les conclusions du sondage. Le responsable de chaque organisme visé par le sondage a reçu copie du questionnaire en février 1995 et y a répondu tard cette même année. Après avoir corrigé les erreurs les plus évidentes, les réponses reçues ont été informatisées et compilées. Bien que les résultats du sondage ne

Suivis

- L'étude d'un échantillon d'ententes de partage de renseignements;
- la mise à jour des calendriers de conservation et d'élimination des renseignements personnels; et
- l'analyse, dans l'optique d'un plus grand respect de la *Loi sur la protection des renseignements personnels*, des démarches actuelles entourant la collecte de renseignements personnels.

Comme à l'habitude, nous sommes penchés sur certaines vérifications antérieures afin de constater à quel point les organismes fédéraux appliquent nos recommandations.

Commission canadienne des droits de la personne La commission s'est attaquée à plusieurs des problèmes soulevés par notre vérification de 1992, dont la description, la conservation et la protection des dossiers (papier ou électroniques) que la CCDP détient. Cette dernière a également instauré des lignes directrices à l'intention de son personnel lors de la communication par télécopieur des renseignements de nature souvent délicate qui découlent des plaintes.

La commission doit cependant poursuivre ses modifications à son système informatique de gestion de cas afin d'y restreindre l'accès sur la base de certains renseignements plutôt que de fichiers complets. De plus, la CCDP doit commencer à clairement indiquer dans ses contrats liant des sous-traitants que les renseignements personnels auxquels ces derniers ont accès relèvent du contrôle exclusif de la commission, même si les sous-traitants s'engagent à en respecter le caractère confidentiel. Enfin, ses listes d'expédition doivent être décrites plus précisément dans *InfoSource*.

Conseil national de recherches Le conseil a appliqué l'ensemble des recommandations découlant de notre vérification de 1992. L'unique exception, soit celle traitant de l'élimination de vieux dossiers, est en cours d'application.

Le CNRC a notamment

- incorporé des clauses de protection des renseignements personnels aux contrats qu'il accorde aux sous-traitants assurant son Programme d'aide aux employés;

Division Huron. Nous avons prévu nous pencher sur un problème soulevé dans notre rapport annuel de l'an dernier, soit le fait que les gestionnaires de la Division Huron conservaient apparemment des dossiers "fantômes" au sujet de leurs employés (auxquels ils leur refusaient l'accès en vertu de la Loi sur la protection des renseignements personnels).

- Lors de sa vérification, le personnel du siège social de la SCP affecté à la protection de la vie privée a confirmé l'existence de ces dossiers "fantômes", et a aussitôt réagi. Les gestionnaires de la SCP se sont vu "autorisés" (et non obligés) à conserver certains documents concernant leurs employés, tels les fiches de présence ou autres papiers essentiels "à la surveillance des employés, particulièrement ceux des sites éloignés", mais ceci à deux conditions :
- que ces documents ne soient que des duplicatas des originaux consignés aux dossiers officiels des employés; et
 - que ces documents soient décrits dans un nouveau fichier de renseignements personnels inscrit au répertoire *InfoSource*.

Suite à notre examen des méthodes de vérification appliquées par la SCP, nous avons conclu que nous en serions arrivés aux mêmes constatations, et que notre propre vérification n'avait des lors plus d'objet. Nous nous pencherons plutôt sur les plaintes reçues à l'endroit de la SCP afin de vérifier l'efficacité des mesures correctives proposées par cette dernière.

Citoyenneté et Immigration Canada

- L'an dernier, notre rapport décrivait nos recommandations suite à la vérification que nous avions effectuée des systèmes informatiques de ce ministère. À l'époque, ce dernier était en pleine réorganisation, refonte majeure dont il n'est toujours pas sorti. Malgré les exigences d'un tel climat de travail, le ministère a cependant mis de l'avant divers plans d'action interne visant à résoudre certains des autres problèmes soulevés par la vérification, tels
- la mise sur pied à grande échelle d'un programme de formation continue en protection de la vie privée;
 - la révision complète de toutes les descriptions contenues dans le répertoire *InfoSource*;

Société canadienne des postes - Division Huron

Alors que le Commissariat s'apprêtait à y effectuer une vérification, la SCP a décidé de prendre les devants et de mener sa propre vérification au sein de sa

conséquence.

Le Centre a très vite réagi aux suggestions précédentes et a pris des mesures en

- publier dans le répertoire *InfoSource* une description exacte des renseignements personnels détenus par le centre.
- former ses employés actuels et futurs aux exigences de la *Loi sur la protection des renseignements personnels*, ainsi qu'aux activités précédentes; et
- faire inspecter la sécurité de son matériel informatique par une équipe spécialisée de la Gendarmerie royale du Canada;
- inscrire à tout contrat liant une tierce partie le fait que les renseignements personnels auxquels cette dernière a accès non seulement relèvent du contrôle du CCG mais sont également assujettis à la *Loi sur la protection des renseignements personnels*;
- faire montre de prudence lors de la communication de renseignements personnels par télécopieur;
- prendre les mesures requises afin de protéger ses renseignements personnels de tout accès interdit;
- collaborer avec les Archives nationales à l'élaboration d'un calendrier de conservation et d'élimination des renseignements personnels qu'il détient, puis vérifier ces derniers afin d'en éliminer ceux qui auraient déjà dû l'être;
- réviser les formulaires dont il se sert, afin tant de ne plus recueillir de renseignements personnels inutiles de la part de ses étudiants que d'informer ces derniers de leurs droits en vertu de la *Loi sur la protection des renseignements personnels*;
- organiser et classer les renseignements personnels qu'il détient, et en contrôler la communication;
- instaurer d'ici un an une politique de gestion de ses renseignements personnels, du moment de leur collecte à celui de leur élimination;

signaux étrangers quelques renseignements reliés à des Canadiens, mais le Centre s'est doté de procédures strictes visant à minimiser ces possibilités et à détruire tout renseignement ne satisfaisant pas aux critères fédéraux. Nos enquêteurs ont également conclu que les rapports que le CST fournissait au gouvernement ne contenaient pas à la *Loi sur la protection des renseignements personnels*.

Le gouvernement devrait cependant adopter une loi habilitant clairement les programmes et activités du CST et précisant leur étendue et leurs limites. Ceci permettrait non seulement d'évaluer avec objectivité les pratiques de gestion des renseignements personnels du CST et d'en légaliser les activités, mais aurait aussi pour conséquence de garantir juridiquement les libertés des Canadiens. Une telle loi provoquerait de plus une discussion éclairée et une meilleure compréhension des activités du CST, dissipant ainsi la chaleur des débats actuels. Le moment semble bien choisi : au moment d'aller sous presse, le gouvernement vient en effet d'annoncer la création d'un organisme indépendant de surveillance du CST.

Centre canadien de gestion

Ce centre, créé en 1991, offre une formation en gestion aux cadres et hauts fonctionnaires fédéraux. Il regroupe environ 200 employés, répartis entre ses deux sites d'Ottawa-Hull et ses bureaux d'Edmonton, et comprenant professeurs, chercheurs et personnel de soutien des secteurs tant public que privé. Les renseignements personnels que détient le CCG visent son personnel ainsi que près de 30 p. cent des quelque 12 000 étudiants participant annuellement aux cours ou conférences du centre (lequel ne recueille aucun renseignement personnel relié aux autres élèves).

Cette toute première vérification du CCG nous a permis de constater les habitudes du centre en matière de collecte, d'utilisation, de communication et de protection des renseignements personnels qu'il détient. Nous avons également pu constater que le personnel du CCG n'était que bien peu au courant de ses obligations en vertu de la *Loi sur la protection des renseignements personnels*, ce qui explique bon nombre des manquements que notre vérification a fait ressortir. Les employés du centre possédaient cependant bien la notion de "confidentialité", et se sont montrés de bons élèves. Nous avons notamment recommandé au CCG ce qui suit :

et électroniques de ces pays. Le CST relève du ministre de la Défense nationale.

Cette vérification s'est révélée être une des plus longues et complexes jamais entreprises par le Commissariat, et ce pour plusieurs raisons. La première en est la nature extrêmement délicate des renseignements recueillis et traités par le CST, qui a signifié l'obtention par nos enquêteurs de cotes de sécurité de haut niveau, ainsi que des modifications à nos locaux et l'acquisition de matériel approprié.

Puis, au cours de la vérification, diverses allégations publiques accusant le CST de recueillir des renseignements sur la population et les partis politiques canadiens ont attiré l'attention sur cet organisme et sur notre vérification, créant par le fait même certaines attentes quant aux conclusions que nous en pourrions tirer de cette dernière.

Troisièmement, la *Loi sur les secrets officiels* limite les révélations que peut faire le Commissaire à la protection de la vie privée, qui y est assujéti.

La dernière raison, la plus pertinente en ce qui nous concerne, est le flou qui entoure le mandat du CST, lequel n'est contenu dans aucune loi habilitante (contrairement à la majorité des organismes fédéraux), à l'exception toutefois des dispositions assez vagues qui visent le ministre en vertu de la *Loi sur la défense nationale*. Nos vérifications se fondent généralement sur les mandats des organismes où nous oeuvrons, nous permettant ainsi de mieux évaluer leur respect de la *Loi sur la protection des renseignements personnels* puisque nous pouvons alors mieux déterminer la façon dont ces organismes recueillent, utilisent, communiquent et éliminent les renseignements personnels qu'ils utilisent, ainsi que la nature de ces renseignements. Le rôle du CST lui a été confié d'office plutôt que par le biais d'une loi, et c'est en fonction de ce mandat d'office que nous avons dû travailler.

Se fondant sur un échantillonnage représentatif des renseignements et des rapports générés par le CST, nos enquêteurs en ont conclu que le Centre ne recueillait que les renseignements qui lui sont permis en vertu des critères fédéraux de surveillance de pays étrangers. Il ne semble y avoir aucun fondement aux allégations voulant que le CST "espionne des Canadiens" ou surveille leurs communications. Il est inévitable que le CST recueille lors de sa surveillance de

DRHC (bis) : échange électronique de renseignements sur l'emploi

Le ministère vient de mettre sur pied un système permettant de rapprocher électroniquement les gens des emplois qu'ils recherchent. Ce système, branché sur l'Internet et en version pilote dans la région d'Ottawa, établit des liens entre les postes à combler par les employeurs (qui en décrivent les responsabilités, les compétences et l'expérience requises) et les personnes recherchant un emploi (en fonction de leurs antécédents scolaires et professionnels). DRHC nous a impliqués au chapitre de la collecte et de la conservation des renseignements reliés aux antécédents des demandeurs d'emploi, ainsi que de l'utilisation ultérieure de ces renseignements personnels à des fins d'études du marché de l'emploi.

Vérifications

La Loi sur la protection des renseignements personnels confère au Commissaire à la protection de la vie privée le pouvoir (et le loisir) de mener enquête sur la façon dont le gouvernement fédéral respecte les pratiques de gestion équitable qu'énonce la Loi quant à la collecte, l'utilisation, la communication et l'élimination des renseignements personnels détenus par un organisme fédéral.

Après avoir, le Commissariat choisissait un certain nombre d'organismes (ou de programmes dans le cas de gros organismes) au sein desquels mener enquête. La quasi-impossibilité d'effectuer des vérifications systématiques oblige cependant le Commissariat à s'intéresser de plus en plus aux enjeux affectant l'ensemble de la fonction publique fédérale.

Nous avons quand même effectué deux vérifications cette année, soit au sein du Centre de sécurité des télécommunications et du Centre canadien de développement des ressources humaines. Une troisième vérification, menée à l'intérieur par la Division du centre de la Société canadienne des postes, nous a été soumise pour contrôle.

Centre de sécurité des télécommunications

Le Centre fournit au gouvernement fédéral les conseils et les outils lui permettant d'assurer la sécurité de ses communications, ainsi que des services de collecte et d'analyse de signaux provenant de puissances étrangères. Ces services se traduisent par l'interception et l'étude des communications radiophoniques, radar

Commission de la fonction publique : clauses dans les contrats de sondage

Suite aux recommandations de notre gestionnaire de portefeuille, la Commission de la fonction publique a accepté d'incorporer à ses contrats liant des entreprises privées des clauses assujettissant ces dernières à la *Loi sur la protection des renseignements personnels*. Notre intervention découlait de la communication à une maison de sondage des noms, adresses et numéros de téléphone des personnes s'étant prévalues des mécanismes d'appel de la Commission, et ce afin d'évaluer leur niveau de satisfaction.

GRC (bis) : suspension de la collaboration

Bien que la sécurité publique préoccupe de plus en plus la population, la Gendarmerie royale s'est ralliée aux arguments du Commissariat à l'effet que les reportages télévisés sur la criminalité devaient respecter le droit des personnes filmées lors de patrouilles policières à être présumées innocentes jusqu'à leur comparution devant les tribunaux. La GRC a donc suspendu sa collaboration à l'émission *To Serve and Protect*, tournée en Colombie-Britannique, jusqu'à ce que ses réalisateurs acceptent comme il se fait déjà aux États-Unis de cacher les visages, adresses et plaques d'immatriculation des personnes filmées. La GRC a de plus accepté d'établir une politique nationale régissant sa collaboration à tout projet communautaire ou des médias de lutte contre le crime.

Développement des ressources humaines Canada : l'Internet

Eh oui! Le gouvernement fédéral a maintenant pignon sur l'Internet. Mais cette ouverture informatique relance de plus belle la question de la sécurité entourant nos renseignements personnels. Développement des ressources humaines, ce ministère qui détient des renseignements sur l'ensemble de la population active canadienne, a innové en établissant la toute première politique fédérale visant l'usage de l'Internet pour la prestation de ses services. Nous nous y sommes impliqués, notamment au chapitre de la protection des renseignements fournis par les citoyens accédant le site Web de DRHC, et de la transmission (maintenant interdite) de renseignements personnels par le biais de l'Internet. (Notre propre site Web dépend d'ordinateurs dédiés à cette fin et indépendants de notre réseau interne.) La politique de DRHC devrait se révéler un modèle utile pour tout autre organisme fédéral désireux d'en faire autant (voir aussi *L'Internet et votre vie privée : petit guide de l'usager*).

Travaux publics et Services gouvernementaux Canada : informatisation du processus de vérification des antécédents

visés soient prévenus de l'examen de leurs relevés d'appels, et que ces relevés n'indiquent pas les quatre derniers chiffres des numéros signalés afin de protéger l'anonymat des personnes appelées. Nous n'oublions pas non plus qu'un tel relevé peut être tout à fait inutile dans le cas d'un employé travaillant pour un organisme répondant à des appels téléphoniques de partout au pays.

La vérification des antécédents de chaque nouvel employé ou sous-traitant du gouvernement fédéral représente une tâche énorme (près de 29 000 enquêtes par année, selon Travaux publics et Services gouvernementaux). Le ministère a donc décidé de simplifier et d'informatiser le processus en concevant un nouveau système automatisé de collecte de renseignements pour fins d'enquêtes de sécurité qui lui fera économiser bien du papier et du temps.

Ce nouveau système repose sur un logiciel permettant aux entreprises privées traitant avec le gouvernement fédéral de recueillir et de transmettre des renseignements personnels au sujet des employés requérant une cote de sécurité. Ces entreprises peuvent installer ce logiciel dans un de leurs ordinateurs, recueillir les renseignements requis et les acheminer en direct à TP&SGC. Ces entreprises feront partie des 26 000 organismes privés et publics auxquels le ministère offrira d'utiliser le système.

Vu la quantité et de la nature des renseignements (antécédents familiaux et professionnels) qu'acheminerait le système, ainsi que l'absence de lois protégeant la vie privée au sein du secteur privé, le transfert de la responsabilité de la collecte et de l'entreposage de ces renseignements à des entreprises privées nous préoccupait.

Le ministère nous a alors soumis le projet d'entente de sécurité qui lierait les entreprises autorisées à recueillir et à entreposer les renseignements précédents. Cette entente confirmerait les droits fédéraux de propriété des renseignements, et obligerait les entreprises à assurer la protection de ces derniers conformément aux dispositions de la Politique gouvernementale sur la sécurité. TP&SGC en est actuellement à tester le système au sein d'un groupe pilote.

d'un ancien mineur au radon. La Commission ontarienne évalue alors les allocations qu'elle versera à ceux atteints d'un cancer du poumon;

- que les travailleurs ont le droit de prendre connaissance des renseignements les concernant, lesquels seront versés dans un fichier distinct par la CCEA. Ce fichier servirait de précédent pour le cas où d'autres mines d'uranium fermeraient leurs portes.

Rideau Hall : vérification du casier judiciaire des candidats à l'Ordre du Canada

Les responsables de la Chancellerie de Rideau Hall nous ont demandé au printemps 1995 s'ils pouvaient vérifier les casiers judiciaires des personnes qui leur sont suggérées pour l'octroi de l'Ordre du Canada, dont le respect pouvait souffrir de la réputation entachée de l'un de ses membres. Nous leur avons alors suggéré un compromis qui répondrait à leurs besoins tout en respectant la vie privée des candidats. Une fois prévenus de leur statut, ces derniers se verraient demander d'obtenir de la Gendarmerie royale du Canada qu'elle confirme l'absence de casier judiciaire à leur nom. Les candidats pourraient également, s'ils le préfèrent, autoriser la Chancellerie à effectuer cette vérification en leur nom. Ils pourraient évidemment refuser de se plier à cette vérification, ce qui pourrait entraîner le retrait de leur candidature.

Gendarmerie royale du Canada : élimination de renseignements personnels

Depuis notre dernier rapport annuel, dans lequel nous rapportions avoir trouvé des renseignements personnels de la Gendarmerie royale dans un coffre-fort acheté à une vente de matériel gouvernemental excédentaire, la GRC a demandé à notre gestionnaire de portefeuille de réviser la section qu'elle avait rajoutée à son manuel interne sur la sécurité visant à s'assurer que son personnel vidèrait désormais tout meuble excédentaire destiné à la vente.

Centre de recherches sur les communications : relevés d'appels des employés

Les agents de télécommunications du Centre (affilié à Industrie Canada) nous ont demandé de les aider à définir dans quelles circonstances les gestionnaires du CRC pouvaient consulter les relevés des appels faits par leurs employés. L'objectif des gestionnaires étant de justifier certains frais ou de confirmer des exagérations au chapitre des appels interurbains, nous avons suggéré au CRC que les employés

- Au Canada, la réglementation de l'énergie atomique incombe à la Commission et comprend l'étude des effets des substances radioactives sur la santé des travailleurs. Par conséquent, la CCEA exige des compagnies exploitantes de mines d'uranium qu'elles se documentent sur les effets du radon, un gaz cancérogène, sur ceux de leurs mineurs y ayant été exposés.
- La Commission avait demandé à la Dennison de lui faire parvenir ces dossiers, préférant que cette dernière ne détruise pas des documents aussi importants pour la recherche des effets à long terme du radon. La Dennison ayant accepté, la CCEA s'est alors penchée sur la légalité, aux termes de la Loi sur la protection des renseignements personnels, de la collecte et de l'utilisation de ces dossiers.
- La Commission souhaite coupler ces renseignements avec les données statistiques fédérales sur la mortalité au pays afin de déterminer les effets du radon sur l'espérance de vie des travailleurs ainsi que leur taux de mortalité provoquée par le cancer du poumon. Cette utilisation des renseignements est conforme aux fins de leur collecte originale par la Dennison, soit l'étude des effets de substances radioactives sur la santé.
- S'assurant que la nouvelle base de données de la Commission répondait aux exigences de la Loi, le gestionnaire de portefeuille a confirmé :
- que la recherche visée par la CCEA relève de son rôle de contrôle des incidences des substances radioactives sur la santé et la sécurité;
 - que les renseignements avaient été à l'origine recueillis directement auprès des travailleurs concernés (bien que la CCEA les ait quant à elle recueillis indirectement de la Dennison). (L'obtention par la CCEA du consentement de chacun des travailleurs aurait posé de nombreuses difficultés, l'ensemble de ces derniers ayant quitté Elliot Lake avant la fermeture de la mine);
 - qu'il existe un calendrier de conservation des renseignements, desquels la CCEA n'entend pas se débarrasser avant que le plus jeune des mineurs (présupposé âgé de 18 ans à son embauche) ne devienne centenaire;
 - qu'un des usages actuels des renseignements par la CCEA est conforme aux fins de la collecte originale, soit la confirmation, sur demande de la Commission ontarienne des accidents du travail, de l'exposition antérieure

Le nouveau système de portefeuilles de la Direction a fonctionné à pleine capacité cette dernière année. Nous avons consacré moins de temps à des vérifications et des suivis formels, et bien davantage à dialoguer avec les représentants des divers ministères et à les conseiller, fidèles en cela à la tendance actuelle qui prône une activité accrue et un attachement au service.

Il est désormais de plus en plus fréquent de voir nos gestionnaires de portefeuille impliqués dès les débuts du concept d'un programme ou d'une activité fédérale. Dans certains cas, nous participons même aux délibérations de comités ministériels pilotant de nouveaux dossiers : à preuve nos efforts auprès du Directeur général des élections sur son projet de liste électorale permanente (voir *Voter librement?* en page 15), et auprès du ministère de la Justice quant à son nouveau registre des armes à feu. Tel qu'illustré dans les pages suivantes, nos gestionnaires de portefeuille ont à cœur d'éviter les problèmes au lieu de les résoudre.

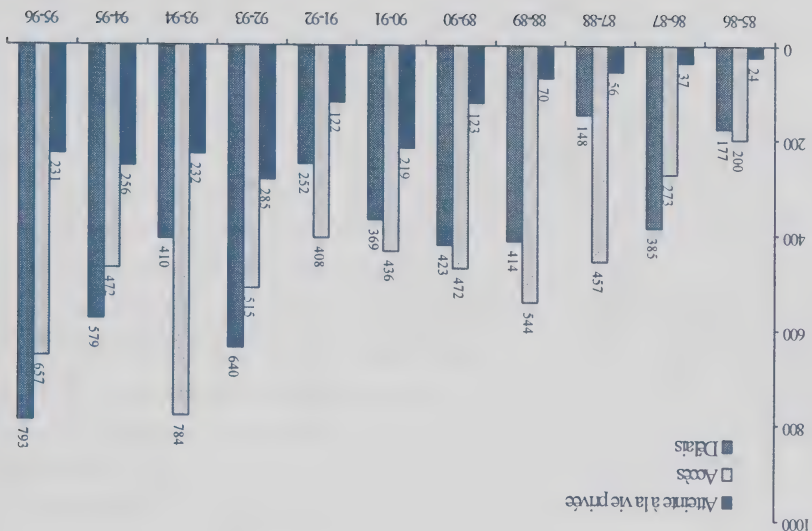
Mieux vaut prévenir...

Il ne suffit pas d'effectuer des vérifications pour s'assurer que les organismes fédéraux se conforment à la *Loi sur la protection des renseignements personnels*. En effet, notre rôle de conseiller est tout aussi important, et il est crucial que nous le remplissions le plus tôt possible. Les organismes fédéraux sont de plus en plus nombreux à reconnaître les avantages d'impliquer nos gestionnaires de portefeuille dès les débuts d'un projet, que celui-ci soit l'élaboration d'une nouvelle politique ou le lancement d'un programme pouvant affecter la vie privée d'employés ou de clients. Voici certains des nombreux dossiers sur lesquels nos gestionnaires de portefeuille se sont penchés cette année.

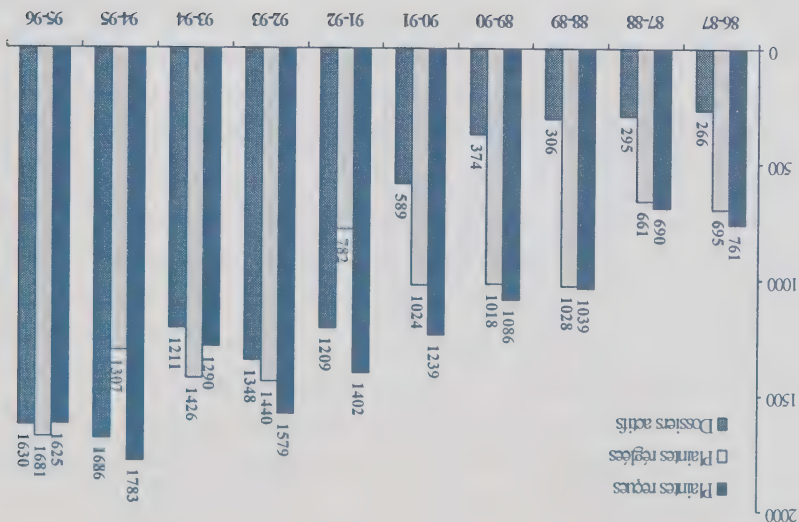
Commission de contrôle de l'énergie atomique : exposition de mineurs au radon

Suite à la fermeture de la mine Dennison d'Elliot Lake, la Commission nous a demandé conseil quant à la requête des dirigeants de la mine de détruire leurs dossiers de suivi des mineurs ayant été exposés au radon (la Dennison ayant pratiqué l'extraction de l'uranium à Elliot Lake durant les années cinquante et soixante).

Plaintes réglées et motifs 1986-96



Plaintes 1986-96



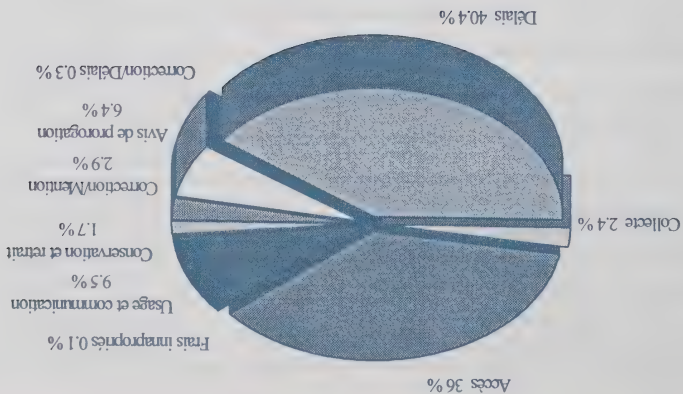
Plaintes réglées pas institutions et résultats

Institution	#	Fondée	Fondée; résolue	Non fondée	Aban- donnée	Résolue
Enquêteur correctionnel Canada, L'	4	1	1	1	1	0
Environnement Canada	5	1	0	3	1	0
Gendarmerie royale du Canada	136	19	11	85	15	6
Industrie Canada	6	1	0	3	2	0
Industrie, Science et Technologie	1	0	0	1	0	0
Justice, Ministère de la	19	2	2	15	0	0
Ministère du patrimoine	3	1	0	2	0	0
Monnaie royale canadienne	4	0	2	2	0	0
Office de com. du poisson d'eau douce	2	0	0	2	0	0
Office national du film	5	1	3	1	0	0
Pêches et Océans	4	1	0	3	0	0
Ressources naturelles Canada	3	1	1	1	0	0
Revenu Canada - Impôt, douanes et accise	253	171	10	66	5	1
Santé Canada	22	4	5	10	0	3
Service canadien du renseignement de sécurité	101	0	0	101	0	0
Service correctionnel Canada	305	106	31	152	10	6
Société canadienne d'hypothèques et de logement	2	0	0	2	0	0
Société canadienne des Ports	2	0	1	1	0	0
Société canadienne des Postes	41	10	10	18	1	2
Société du crédit agricole Canada	3	0	2	1	0	0
Solliciteur général Canada	3	0	0	3	0	0
Statistiques Canada	1	0	0	1	0	0
Transports Canada	15	3	1	10	0	1
Travail Canada	2	0	0	2	0	0
Travaux publics et Services gouv. Canada	21	1	7	9	1	3
TOTAL	1,681	638	154	764	97	28

Plaintes réglées pas institutions et résultats

Institution	#	Fondée	Fondée; résolue	Non fondée	Aban- donnée	Résolue
Affaires étrangères et Commerce int. Canada	5	3	0	2	0	0
Affaires indiennes et du Nord Canada	1	0	1	0	0	0
Agence canadienne de développement int.	4	1	0	2	1	0
Agence de promotion écon. du Canada	1	1	0	0	0	0
Agriculture et Agro-alimentaire Canada	33	4	5	22	1	1
Anciens combattants Canada	3	0	0	3	0	0
Archives Nationales du Canada	32	5	3	23	1	0
Banque fédérale de développement	1	0	1	0	0	0
Bibliothèque nationale du Canada	2	0	2	0	0	0
Bureau de l'inspecteur général du Canada	1	0	0	1	0	0
Bureau du Conseil Privé	1	1	0	0	0	0
Bureau du vérificateur général du Canada	2	0	1	1	0	0
Centre int. des droits de la personne	1	0	0	1	0	0
Centre national des Arts	1	0	1	0	0	0
Citoyenneté et immigration Canada	143	95	11	26	10	1
Commissariat aux langues officielles	7	3	0	4	0	0
Commission canadienne des droits de la personne	4	0	0	3	0	1
Com. de l'immigration et du statut du réfugié	22	2	17	1	2	0
Commission de la capitale nationale	1	0	0	1	0	0
Commission de la fonction publique du Canada	7	0	1	4	2	0
Com. des plaintes du public contre la GRC	2	2	0	0	0	0
Commission nat. des libérations conditionnelles	17	1	4	12	0	0
Conseil des arts du Canada	1	1	0	0	0	0
Conseil du Trésor du Canada, Secrétariat	1	0	0	1	0	0
Conseil national de recherches Canada	4	0	0	4	0	0
Consommateurs et des Sociétés Canada	2	1	0	1	0	0
Défense nationale	316	171	12	90	40	3
Développement des ressources humaines Canada	102	24	8	66	4	0
Elections Canada	1	0	0	1	0	0
Emploi et Immigration Canada	0	0	0	0	0	0

Plaintes réglées par motifs



Origine des plaintes réglées

Terre-Neuve	15
Ile-du-Prince-Édouard	14
Nouvelle Écosse	50
Nouveau Brunswick	34
Québec	172
Région de la capitale nationale - Québec	17
Région de la capitale nationale- Ontario	349
Ontario	510
Manitoba	32
Saskatchewan	49
Alberta	132
Colombie-Britannique	293
Yukon	2
Hors Canada	12
TOTAL	1,681

Les dix ministères les plus visés selon les plaintes reçues

Motifs					
Ministère	Total	Accès	Délais	Vie privée	
Service correctionnel Canada	312	113	157	42	
Défense nationale	267	83	162	22	
Revenu Canada	235	58	141	36	
Gendarmerie royale du Canada	138	82	23	33	
Citoyenneté et immigration Canada	106	31	67	8	
Service canadien du renseignement de sécurité	90	82	6	2	
Développement des ressources humaines Canada	80	33	22	25	
Conseil du trésor du Canada, Secrétaire	67	3	0	64	
Société canadienne des Postes	46	27	0	19	
Archives nationales du Canada	41	25	5	11	
AUTRE	243	141	53	49	
TOTAL		1,625	678	636	311

Plaintes réglées par motifs et résultats

		Résultats				
Motifs	Accès	Fondée	Fondée; résolue	Non fondée	Résolue	Abandon-née
		12	126	470	21	28
Accès	12	119	430	19	26	606
Correction/Annotation	0	7	39	1	2	49
Frais contre-indiqués	0	0	1	1	0	2
Répertoire	0	0	0	0	0	0
Langue	0	0	0	0	0	0
Atteinte à la vie privée	42	25	140	7	17	231
Collecte	2	0	36	1	2	41
Conservation/Retrait	10	6	9	2	2	29
Usage/Communication	30	19	95	4	13	161
Délais	584	3	154	0	52	793
Correction/Délai	2	0	2	0	1	5
Délais	521	3	119	0	37	680
Avis de prorogation	61	0	33	0	14	108
TOTAL	638	154	764	28	97	1,681

Où sont les formulaires d'accès à des renseignements personnels? Des dizaines de personnes se sont plaintes au Commissariat de ce qu'elles ne pouvaient pas trouver de formulaire de demande d'accès à des renseignements personnels. Certaines s'étaient présentées dans des bureaux de poste, d'autres à des Centres d'emploi du Canada, deux endroits où ces formulaires sont logiquement disponibles aux dires du Conseil du Trésor, responsable de leur distribution. Nous signalons généralement ces problèmes au Conseil dès que nous en sommes conscients, mais d'ici leur résolution, nous faisons parvenir chaque année des milliers de formulaires à la population.

Ces formulaires, ainsi que le répertoire *InfoSource* qu'ils citent, devraient normalement être disponibles dans les centres d'emploi, les bibliothèques et salles de lecture fédérales, les grandes bibliothèques publiques et universitaires, les bureaux de comté des députés et les locaux des conseils de bande autochtones.

Demandes de renseignements 1986-96



Demandes de renseignements

Beaucoup de personnes nous contactent que nous ne pouvons malheureusement pas aider parce que le sujet abordé ne relève pas de notre compétence mais de celle du secteur privé (banques, compagnies d'assurances, sociétés de transport). Plusieurs individus protestaient violemment contre Sprint Canada, dont les employés leur demandaient leur numéro d'assurance sociale. D'autres s'objectaient à ce que la gestion de Purolator Courrier prenne les empreintes digitales de tous ses employés. De nombreux employés d'Air Canada voulaient que nos enquêteurs se penchent sur les pratiques de cette société en termes d'accès aux dossiers et aux messages électroniques de son personnel.

En outre, même si ce sont d'anciennes sociétés de la Couronne, ni Air Canada ni Via Rail (également le sujet de plusieurs appels) ne sont assujetties à la Loi fédérale sur la protection des renseignements personnels. Les employés n'ont aucun droit juridique à consulter leurs dossiers du personnel à moins que leur convention collective ne contienne une entente à ce chapitre.

OC Transpo

Plusieurs appels provenant d'employés d'OC Transpo qui s'étaient vu refuser accès à leurs dossiers illustrent bien le statut plutôt inhabituel de cette société outaouaise de transport en commun. Ses parcours incluant la ville québécoise de Hull en font un service interprovincial, donc de compétence fédérale. Cependant, OC Transpo n'est assujettie ni à la Loi sur la protection des renseignements personnels ni à la loi ontarienne équivalente.

Le Commissaire à la protection de la vie privée de l'Ontario nous a informé qu'OC Transpo tentait toutefois de respecter cette dernière loi. Ce Commissaire a en effet obtenu accès aux dossiers des employés de la société, à l'exception cependant des cas de harcèlement ou de grief, pour lesquels les responsables d'OC Transpo refusent de permettre l'étude des documents.

Le NAS des cartes d'assurance-vieillesse

Trois individus ont protesté du fait que leur numéro d'assurance sociale apparaissait sur leur carte d'assurance-vieillesse. Cette carte est utilisée régulièrement comme pièce d'identité par les personnes âgées. Ainsi, afin d'obtenir un rabais d'un magasin à rayons, elles doivent présenter cette carte aux commis, qui obtiennent alors leur NAS. Bien qu'aucun des trois individus ne se soit plaint de façon formelle ("pour ne pas réveiller le chat qui dort" selon l'un d'eux), une autre personne a officiellement porté plainte à cet effet de sorte que le Commissariat se penche quand même sur le dossier.

ses opérations de courrier et mène maintenant des vérifications de routine pour éviter que de telles erreurs ne se reproduisent.

Les lignes directrices pour les employés de Revenu Canada fonctionnent

L'année dernière, nous rapportions l'établissement de lignes directrices de Revenu Canada visant l'utilisation des déclarations de revenus de ses employés à des fins de supervision et d'évaluation de leur rendement. Cette année, un employé s'est plaint de ce que le ministère avait enfreint ces lignes directrices en se servant de ses déclarations de revenus pour le congédier.

L'enquêteur, suite à son examen des dossiers de l'employé, a découvert que l'employé et le gestionnaire de ce dernier avait à maintes reprises discuté de son comportement, de ses absences du bureau et de la fréquence de ses appels téléphoniques personnels. Préoccupé de la faible productivité de l'employé et de son emploi du temps au travail, le gestionnaire avait demandé une vérification des Affaires internes.

La vérification a retracé l'employé alors qu'il accédait à d'importantes données—partielles, et non des déclarations complètes—du système informatique de RC. La vérification a prouvé que l'employé avait accédé de façon non autorisée à ses propres déclarations de revenus, ainsi qu'à celles de plusieurs membres de sa famille et d'une connaissance, aucune n'étant cependant nécessaire à son travail. La vérification a également permis d'établir que l'employé, pourtant rémunéré, n'avait pas déclaré ses revenus depuis plusieurs années.

Les vérificateurs ne se sont pas volontairement concentrés sur les déclarations de revenus de l'employé, mais ont plutôt simplement suivi la piste qu'il avait laissée dans le système informatique. Il n'y avait aucun renseignement fiscal dans ses dossiers personnels. Et si Revenu Canada a finalement congédié l'employé, les raisons en sont ses habitudes de travail, son manque de productivité et son accès non autorisé à ses propres renseignements et à ceux des autres. Le ministère lui a de plus demandé de soumettre des déclarations de revenus pour les années manquantes.

Le Commissaire a conclu que la plainte n'était pas fondée. Si le gestionnaire avait délibérément décidé d'étudier les déclarations de revenus de l'employé, les lignes directrices auraient exigé qu'il fournisse des justifications suffisantes et qu'il en obtienne l'autorisation du sous-ministre adjoint.

Le personnel des affaires publiques du MDN fait des révélations aux médias
Le personnel des affaires publiques gouvernemental est souvent pris entre deux
feux : il est soit trop discret, soit pas assez, ainsi qu'en témoigne ce cas d'une
famille accusatrice.

Un jeune soldat meurt dans des circonstances tragiques, et ses parents exercent
des pressions pour obtenir pus de détails sur ces dernières. Insatisfaits des
explications que leur fournit le ministère de la Défense nationale, ils se tournent
vers les médias, auxquels les responsables des affaires publiques du ministère
confient alors les problèmes d'alcool du soldat et les efforts qui ont été faits pour
lui venir en aide. Dans une autre entrevue, on apprend également du personnel
des affaires publiques que le soldat n'avait pas nommé ses parents comme
personnes à appeler en cas d'urgence.

Les vidéocassettes des entrevues télévisées prouvent deux de ces cas de
communication, que le Commissaire a jugée abusive. Contrairement aux
allégations de la famille, certains détails publiés par un journaliste de la
presse décollaient de l'une des entrevues télévisées et non du personnel des
affaires publiques du MDN.

Le MDN reverra ses procédures internes et tiendra des sessions d'information à
l'intention de son personnel des affaires publiques quant au traitement des
demandes des médias visant des renseignements personnels.

Deux erreurs humaines font aboutir du courrier à une mauvaise adresse

Dans un premier cas, la carte de changement d'adresse d'un individu, adressée au
facteur local de la Société canadienne des postes afin de faire intercepter et suivre
son courrier, a été livrée à son ancien propriétaire. La SCP s'est excusée de cet
incident isolé.

Le deuxième cas a failli être beaucoup plus grave. Une lettre des services de
vérification de Revenu Canada à une contribuable avait été incluse par erreur dans
du courrier expédié à une tierce personne. La lettre, qui contenait des
renseignements au sujet des déclarations de revenus de la contribuable, a
heureusement été renvoyée à Revenu Canada.

Le bureau de Revenu Canada (Impôts) de l'est de Toronto assure apparemment
l'envoi du courrier de la direction des services de vérification. Le personnel
affecté au courrier avait par erreur mélangé la lettre destinée à la contribuable
avec d'autres documents. Le ministère s'est excusé auprès de la dame, a modifié

Les députés n'ont pas de privilège particulier

Une personne s'est plainte de ce qu'un employé de Citoyenneté et Immigration Canada avait communiqué de façon abusive des renseignements personnels à son sujet à un député. L'enquête a confirmé qu'un agent d'immigration avait écrit à un député pour lui décrire le statut d'immigrant et le dossier criminel de la personne.

La Loi sur la protection des renseignements personnels autorise les ministères à communiquer les renseignements personnels de quelqu'un à un député avec le consentement de l'individu si cela lui permet de résoudre un problème de cette personne. Mais les députés ne jouissent pas pour autant d'un droit d'accès particulier aux dossiers des gens. Dans le cas présent, le député ne venait pas en aide à la personne concernée et agissait plutôt au nom de l'ex-conjointe du plaignant. Le ministre n'avait ni le consentement du plaignant pour communiquer ses renseignements personnels au député, ni de raison de le faire. Le Commissaire à la protection de la vie privée a donc jugé que C&IC avait communiqué ces renseignements de façon abusive.

Malheureusement, les renseignements personnels ne peuvent pas être retirés une fois divulgués. On ne peut pas réparer le tort que cela cause à une personne. Cependant, le ministre a assuré le Commissaire que semblable incident ne se reproduirait pas. Les gestionnaires ont accepté d'élaborer et de distribuer une politique qui situerait davantage les responsables chargés de répondre aux demandes des députés au sujet de leurs clients.

Un surveillant part, mais son ordonnateur (et ses dossiers) restent

Suite au départ de son surveillant, un employé de Santé Canada hérite de son ordonnateur... et du rapport d'évaluation de rendement d'un collègue, resté sur le disque rigide de l'ordonnateur. L'employé a fait part de sa trouvaille aux officiels du ministère.

Santé Canada a effacé le document, présenté ses excuses au plaignant, et émis une directive à tout son personnel sur l'importance de vérifier les disques rigides avant de les transférer à des collègues.

Malheureusement, on ne peut pas remettre au collègue les aspects de sa vie privée qu'il a perdus. Ce cas devrait servir d'exemple pour tous ceux qui conservent des renseignements personnels sur leur ordonnateur sans s'arrêter à penser aux conséquences à long terme de leur geste : sans coup de pouce de la part de leur gardien, ces appareils n'oublient jamais rien...

Un sondage sur le marché du travail n'est pas obligatoire

L'enquête n'a pas permis de retrouver cette lettre ni une mention quelconque la concernant dans le journal de l'ordonnateur. Puisque Revenu Canada tentait de percevoir des impôts qui lui étaient dûs, ne savait pas qu'elle avait quitté son emploi, et est investi de pouvoirs précisés dans la *Loi sur l'impôt sur le revenu*, le Commissaire a conclu que l'envoi de l'avis de saisie ne constituait pas une communication abusive de renseignements.

Les sondages de Statistique Canada provoquent toujours des appels au Commissariat. Une dame de Montréal s'est plainte de ce qu'un sondage sur le marché du travail de Statistique Canada exigeait de nombreux renseignements personnels qu'elle devait apparemment fournir. Elle s'opposait aussi à ce qu'on lui demande accès à ses déclarations de revenus à venir, de même qu'à fournir son numéro de téléphone ou celui d'un membre de sa famille ou d'un ami. La dame désirait que le Commissariat l'aide à refuser de répondre aux questions de Statistique Canada.

Ce ministère avait envoyé une lettre d'introduction à la dame avant le sondage afin d'expliquer que celui-ci était réalisé sur une base volontaire. À l'encontre du recensement, les sondages de Statistique Canada ne sont pas obligatoires. Un employé zélé a peut-être tenté de persuader la dame de répondre, ce qui peut avoir donné à cette dernière l'impression qu'elle en était obligée. Cependant, les documents du sondage sont très clairs à cet effet.

L'étude réalisée par Statistique Canada s'échelonne sur six ans au cours desquels les participants sont suivis à intervalles réguliers. Le ministère demande le numéro de téléphone d'un membre de la famille ou d'un ami au cas où il serait impossible de contacter le participant pendant une assez longue période de temps.

La demande d'accès aux déclarations de revenus à venir visait quant à elle à diminuer la tâche des répondants puisque les renseignements financiers demandés s'y retrouvaient déjà. La question était apparemment théorique et visait à évaluer la bonne volonté des participants à accepter une telle communication, laquelle n'a finalement jamais eu lieu.

Le Commissaire a conclu que Statistique Canada avait le pouvoir de réaliser le sondage, que ses buts avaient été clairement expliqués et que la participation y était tout à fait volontaire. Statistique Canada a choisi de ne plus déranger la dame, bien que rien ne puisse garantir que son nom ne soit pigé au hasard lors de prochains sondages.

collègues. Le ministre recueille les renseignements afin d'établir la liste d'ordre inverse de mérite qu'il peut dévoiler, ainsi que ses évaluations, aux employés qui portent plainte, et ce dans le but de défendre ses décisions. Bref, la communication des renseignements allait dans le sens original de la collecte, et a satisfait le Commissaire qu'elle respectait la Loi sur la protection des renseignements personnels.

Conservation obligatoire des notes prises par un comité de sélection

Plusieurs membres de la Gendarmerie royale du Canada se sont plaints de ce qu'il leur était impossible d'obtenir les notes d'entrevue prises par les membres de divers comités de sélection. Les membres prenaient des notes manuscrites afin de les aider à évaluer et classer les candidats. Certains membres avaient conservés leurs notes dans leurs propres dossiers pendant six mois, alors que d'autres les avaient détruites après les entrevues selon des instructions qui auraient été émises par des agents de la GRC. Mais toutes les notes ont finalement été détruites et, dans deux cas, l'ont été après une demande officieuse des plaignants mais avant leur demande formelle.

La Loi à l'égard de cette question est claire : tout renseignement personnel utilisé par un organisme fédéral dans le cadre d'une décision administrative concernant un individu est assujéti à la Loi et doit être conservé pendant un minimum de deux ans. Plusieurs membres du comité n'ont soulevé aucune objection à la conservation de ces notes. En fait, les comités de sélection d'officiers de réserve fourniront, à compter de l'an prochain, un compte rendu aux candidats qui exigera probablement que les notes prises par leurs membres soient conservées afin de récapituler les réponses de certaines personnes à des questions précises. La GRC a accepté de modifier sa politique et conservera désormais les notes d'entrevue dans les dossiers du personnel.

Un avis de saisie n'est pas une communication abusive

Une dame de Toronto s'est plainte de ce que l'envoi par Revenu Canada d'un avis de saisie à son ancien employeur pour impôts impayés constituait une communication abusive de ses renseignements personnels. Après avoir tenté plusieurs fois sans succès de percevoir ces impôts (que la dame tentait de réduire en payant par versements), Revenu Canada lui a expédié une lettre "pré-juridique" la sommant de répondre dans les 15 jours. La lettre et un appel téléphonique à son lieu de travail restant sans réponse, Revenu Canada a alors émis un avis de saisie à son employeur. Mais la dame avait entre-temps quitté son emploi et en avait apparemment averti le ministère par écrit.

En plus de s'excuser auprès du plaignant, le ministère a entrepris de mettre à jour ses listes d'envoi et d'informer ses employés des méthodes d'adressage et de distribution de dossiers personnels. En outre, ce cas a servi à sensibiliser le personnel aux conséquences possibles d'égarder des documents. La plainte a été jugée fondée.

La vie privée des détenteurs de prêts en souffrance n'est pas garantie

Toutefois, la plainte n'est pas obligatoirement fondée. La vie privée doit à l'occasion céder le pas à d'autres exigences dont celle que les Canadiens ont de s'acquitter de leurs dettes. Comme au cours des années précédentes, nous avons été saisis de plaintes à l'endroit de Développement des ressources humaines Canada, dont le personnel communiquait, semble-t-il de façon abusive, à des agences de recouvrement des renseignements concernant des prêts étudiants du Canada en souffrance.

Le gouvernement est non seulement en droit, mais a aussi l'obligation de percevoir ce qui lui est dû. Ne disposant pas de sa propre agence de recouvrement il sous-traite cette fonction à des agences privées. Cela ne viole pas la *Loi sur la protection des renseignements personnels*, et le Commissariat s'assure que le ministère en respecte les dispositions ayant trait à la collecte, l'utilisation et la communication des renseignements personnels.

Des résultats d'heureux candidats sont montrés à des employés excédentaires

Les mises à pied du gouvernement ont provoqué une plainte, non pas de la part d'un employé déclaré excédentaire, mais plutôt d'un employé à qui un poste avait été offert. Ce dernier s'est plaint de ce que le personnel de Travaux publics et Services gouvernementaux Canada avait montré son évaluation à un candidat qui avait échoué afin de justifier sa préférence pour le nouvel employé.

Afin de déterminer qui remplirait les postes, le ministère avait développé des critères de sélection, élaboré des questions et établi un guide de classement ainsi qu'une méthode d'évaluation pour chaque tâche. Il en avait alors établi une liste de candidats en ordre inverse de mérite. Selon le nombre de postes à combler, les employés ont reçu une offre d'emploi ou ont été déclarés excédentaires. Les employés qui avaient échoué et qui avaient intenté un grief à l'endroit du processus obtenaient alors accès aux évaluations des personnes situées plus haut sur la liste de mérite.

Cette communication découle d'une politique de la Commission de la fonction publique visant à s'assurer que le processus est équitable. Les employés sont alors en mesure de vérifier qu'ils ont été correctement évalués selon les critères et leurs

Simultanément, la Direction a accru ses normes de qualité du service afin de réduire le temps et les efforts consacrés aux enquêtes de plaintes et a créé une nouvelle section affectée au traitement des plaintes en retard. Enfin, un autre groupe se penche sur les plaintes de collecte, d'utilisation, de divulgation et de destruction abusives de renseignements personnels (articles 4 à 8 de la Loi sur la protection des renseignements personnels).

C&IC est mis hors jeu

À trois reprises, un entrepreneur en construction de Vancouver a renvoyé au bureau local de Citoyenneté et Immigration Canada des dossiers d'immigration qui lui étaient parvenus par erreur. Lorsque l'incident s'est reproduit une quatrième fois, l'entrepreneur a perdu patience et a expédié le paquet au journal local de Vancouver, *The Province*.

Il semble que l'incident découle de la fermeture du bureau de C&IC à Surrey. Sans nouvelle adresse, le courrier de première classe continuait d'être acheminé au local "CIC" le plus près dans Vancouver Ouest, en l'occurrence "CIC Construction".

Le journaliste a communiqué avec les bureaux du ministère à Vancouver. La réaction ne s'est pas fait attendre. Un gestionnaire a récupéré le dossier, contacté C&IC à Montréal afin de faire rectifier l'adresse, et communiqué avec le service de messagerie qui a reconnu que son personnel aurait dû soit renvoyer les enveloppes soit obtenir des instructions de l'expéditeur. Le gestionnaire a accepté d'être interviewé et photographié, mais a demandé au journaliste de ne pas identifier le sujet du dossier d'immigration dans son article. Le journaliste a accepté, mais il avait déjà appelé la personne concernée afin de lui demander ses réactions et son statut d'immigrant. Vexé, et avec raison, la victime de cette erreur du ministère a porté plainte auprès du Commissaire.

Le dossier, qui contenait des photographies de la victime, ses empreintes digitales, ainsi que ses déclarations assermentées au sujet de ses antécédents politiques et de ses raisons pour demander asile au Canada, avait été communiqué de façon abusive. En dépit de trois essais antérieurs, C&IC n'était pas parvenu à déterminer pourquoi les dossiers lui étaient renvoyés, ni à prendre de mesures pour assurer l'envoi de renseignements personnels de nature très délicate. S'il l'avait fait, le dossier n'aurait jamais abouti sur le bureau d'un journaliste, lui révélant l'identité de la personne concernée et la soumettant à ses questions. Heureusement, le journal n'a pas envenimé la situation, refusant d'identifier la personne en question dans ses pages.

Un total de 1625 nouvelles plaintes a été enregistré au cours de l'exercice 1995-96. Cependant, quoique 1681 dossiers aient été fermés, quelque 1630 cas ont été reportés au prochain exercice financier, soit l'équivalent de pratiquement toute une année de travail.

Deux éléments ont besoin de clarification et les deux résultent du très grand retard accumulé par le Commissariat au chapitre des plaintes portées à son attention.

Comme toutes les agences gouvernementales, le Commissariat doit composer avec des ressources financières décroissantes. Les coupures systématisées en pourcentage ainsi que l'augmentation annuelle de sa charge de travail ont placé le Commissariat devant l'inévitable beaucoup plus rapidement que d'autres agences plus grandes. Le Commissariat n'est établi que pour mener des enquêtes et n'est donc pas en mesure de rejeter des plaignants ni d'exiger qu'ils paient les services offerts.

S'ajoutent aussi aux coupures budgétaires les exigences croissantes de notre clientèle. Les Canadiens montrent une plus grande sensibilité à ce qui menace leur vie privée; ils ont atteint un certain degré de complexité dans la formulation de leurs plaintes, et ils exigent un plus grand respect de leur droit à la vie privée. En effet, nombre de provinces ont adopté des lois protégeant la vie privée, il existe maintenant dans le secteur privé un code de pratiques normalisées de protection de la vie privée, et les médias nous bombardent continuellement des dangers que représentent les changements technologiques pour la vie privée.

S'il lui devient impossible de répondre aux plaintes et à ses correspondants en temps opportun, le Commissariat devra reconnaître que son existence n'est plus pertinente et que l'application de la justice est sérieusement compromise. Pour faire preuve d'une réelle efficacité, le Commissariat ne devrait jamais traiter plus de 500 plaintes à la fois, soit environ 35 cas par enquêteur.

La seule solution est de rationaliser radicalement l'ensemble des opérations. Pour ce faire, vers les derniers mois de 1995, le Commissariat a revu en profondeur son processus d'enquête, tenant également des rencontres individuelles avec le personnel affecté à la vie privée dans les ministères. Notre nouvelle approche réduira la paperasserie, assouplira nos contacts, éliminera des étapes de révision et permettra une plus grande utilisation du téléphone. Bref, notre traitement plus rapide et plus efficace des plaintes reposera sur la force et la flexibilité du rôle de l'ombudsman.

Des lois protégeant la vie privée

L'année qui vient de s'écouler a été relativement calme au chapitre des nouvelles lois, canadiennes ou autres, protégeant notre vie privée.

La Freedom of Information and Protection of Privacy Act est entrée en vigueur en Alberta le 1^{er} octobre. Elle ne s'applique pour l'instant qu'aux documents du gouvernement provincial, mais elle visera plus tard les gouvernements municipaux et régionaux. En novembre, la *Colombie-Britannique* étendait l'application de sa loi aux documents des organismes professionnels autonomes (tel le Collège provincial des médecins), une première au pays.

Les députés du *Nouveau-Brunswick* ont formé un comité, regroupant tous leurs partis, dont le but sera de proposer une loi détaillée pour remplacer le code provincial de protection de la vie privée actuellement en vigueur. Les *Néo-brunswickois* ont actuellement le droit d'obtenir connaissance des renseignements que détient leur gouvernement à leur sujet, mais pas celui de contester la collecte, l'usage ni la communication de ces renseignements. La *Nouvelle-Écosse* a entamé la révision prévue de la loi qu'elle promulguait en 1993. Et l'*Île-du-Prince-Édouard* reste la seule province à ne disposer d'aucune loi régissant l'accès à l'information ni la protection de la vie privée.

Winnipeg a peut-être une longueur d'avance sur ses consœurs, s'étant dotée en janvier d'un arrêté municipal sur l'accès à l'information. Les résidents peuvent désormais prendre connaissance des renseignements que possède la ville à leur endroit, et les corriger au besoin (la loi manitobaine ne s'applique pas aux documents détenus par les gouvernements municipaux ni régionaux).

À l'étranger, l'*Australie* envisage d'étendre l'application de sa *Privacy Act*, actuellement limitée aux documents fédéraux, au secteur privé. En juillet, le Parlement européen a finalement ratifié la Directive sur la protection des données, laquelle s'applique désormais aux pays membres de l'*Union européenne*. Ces derniers ont d'ici à l'été 1998 pour se doter d'une loi conforme à la Directive ou pour adapter celle qu'ils ont présentement. L'article 25 de la Directive interdit à ces pays (et aux entreprises qui y font des affaires) d'exporter vers un pays hors de l'*Union* des renseignements personnels dont les lois de ce dernier ne garantissent pas une protection adéquate.

Le Canada risque de souffrir d'un désavantage commercial par rapport à d'autres pays : en effet, il ne dispose pas encore de lois nationales protégeant, comme l'exige la Directive, les renseignements personnels détenus tant par les gouvernements que les entreprises privées.

- dix principes directeurs (inspirés du Code de la CSA sur le même sujet) entourant la collecte, l'usage et la communication de renseignements personnels;

- des lignes directrices de la *Canadian Organization for the Advancement of Computers in Health* traitant de la sécurité et du respect de la vie privée dans les systèmes informatiques de santé;

- une politique sur le couplage de données reflétant celle en vigueur à Statistique Canada; et

- une marche à suivre officielle régissant les demandes d'accès aux renseignements détenus par l'ICIS.

Ces nouvelles lignes directrices seront la norme minimale appliquée à tous les renseignements détenus par l'Institut, et entreront en vigueur en 1996-97.

Il reste cependant deux questions en suspens, dont la première est préoccupante. Compte tenu des extraordinaires pouvoirs de surveillance et de couplage qu'une telle base de données ne manquera pas de fournir aux responsables canadiens de la santé, est-il raisonnable de centraliser autant de renseignements médicaux de nature sensible? Et quelles que soient les mesures de sécurité protégeant ce système, une telle concentration de renseignements en accroîtra les chances de fuites.

La seconde question vise la pertinence de confier à l'Institut la responsabilité d'une étude du mode de vie de près de 22 000 foyers canadiens, lesquels seront interrogés sur leurs problèmes médicaux et les usages qu'ils font de notre système de santé. Par le passé, de telles études ne s'effectuaient que sous la protection contraignante de la *Loi sur la statistique* et des dispositions pertinentes de la *Loi sur la protection des renseignements personnels*. Or les lignes directrices de l'ICIS, pour toutes valables qu'elles soient, ne sont pas une loi.

L'Institut canadien d'information sur la santé : une base de données médicales nationale

Nous avons déjà exprimé dans notre rapport annuel de 1993-94 nos préoccupations face à un nouvel organisme dont la principale activité serait de recueillir des renseignements personnels de nature médicale de la part de divers établissements provinciaux pour en tirer des statistiques départementalisées destinées à la recherche. Le Commissaire voulait s'assurer que l'Institut canadien des renseignements sur la santé, ne relevant pas du gouvernement fédéral, n'aurait accès sans obligation à aucun renseignement médical de nature délicate protégé par la *Loi sur la protection des renseignements personnels* (et l'infiniment plus contraignante *Loi sur la statistique*). Il avait alors offert toute l'aide dont il croyait qu'elle permettrait de bien protéger de tels renseignements. Bien que la réaction initiale de l'ICIS ait été peu encourageante, ses responsables ont complètement changé de cap cette dernière année.

Rappel

Jusqu'en 1994, chaque établissement provincial de santé acheminait à Statistique Canada et à Santé et Bien-être social (assujettis à la *Loi sur la protection des renseignements personnels*) les renseignements relatifs à ses admissions, ses traitements et ses décès. Ces renseignements parvenaient également à deux organismes privés, soit le *MIS Group* et le *Hospital Medical Records Institute*, chargés d'en tirer des statistiques départementalisées destinées à la recherche.

Le Conseil national d'information sur la santé avait alors conclu que la situation provoquait un double emploi et des chevauchements de responsabilités. Ses membres avaient par conséquent recommandé le regroupement de toutes les activités essentielles de ces organismes au sein d'une seule agence sans but lucratif (l'ICIS) reconnue par le gouvernement fédéral, et dont le mandat serait de mettre sur pied et de contrôler un système national de renseignements canadiens sur la santé.

À l'été 1995, l'Institut s'est soudain rendu compte de l'importance du respect de la vie privée et a entrepris de se doter de lignes directrices visant les innombrables renseignements médicaux dont il a la charge. Après nous avoir consultés, les responsables de l'ICIS ont publié quatre documents traitant de la confidentialité et de la vie privée, dont l'un, axé sur les renseignements médicaux, comporte les lignes directrices susmentionnées. Ces dernières comprennent notamment :

- **Rappelez-vous que la touche "Delete" ou "Effacer" de votre clavier n'efface pas... vos documents.** En effet, il est encore possible de les récupérer de votre disque rigide ou des systèmes de reprise. Il existe également des logiciels programmés pour récupérer les documents que vous avez effacés;
- **Le nom que vous voyez à l'écran est peut-être un pseudonyme :** nombreux sont les usagers qui en adoptent un, sinon plusieurs;
- **Faites attention en programmant la liste de vos groupes de discussion préférés :** si vous avez cette possibilité, évitez d'y inscrire le nom des groupes auxquels vous ne voudriez pas être associé publiquement;
- **Attention à votre notice biographique en direct :** si vous souhaitez préserver votre anonymat, ne préparez pas de notice et demandez à votre fournisseur de services de vous retirer de son annuaire en direct. Les notices biographiques peuvent faire l'objet d'une recherche globale ou à distance;
- **La création de votre propre site Web vous met à la merci des entreprises de marketing :** cela peut sembler évident, mais beaucoup l'oublient;
- **Faites attention aux risques sociaux :** le harcèlement, le pistage, l'attaque verbale virulente ou l'inondation de votre boîte aux lettres électroniques de messages indésirables, tout cela arrive sur l'Internet. Les femmes étant particulièrement à risque, identifiez-vous électroniquement de façon neutre;
- **Eduquez bien vos enfants :** assurez-vous que vos enfants apprennent également à protéger leur vie privée. Enseignez-leur de ne révéler aucun renseignement sur eux ni sur vous lors de leurs sessions;
- **Servez-vous des outils qui existent :** si la question vous préoccupe, utilisez des outils technologiques qui vous permettent de protéger votre privée, dont :
 - le chiffrement, qui vous permet de transformer vos messages électroniques ou vos fichiers en des documents inintelligibles pour quiconque (dont votre fournisseur de services) n'est pas le destinataire de vos messages. Il existe sur l'Internet de nombreux logiciels de chiffrement (dont *Pretty Good Privacy* ou *PGP*);
 - les entreprises d'acheminement anonyme de messages, qui disposent d'un serveur qui intercepte votre message et en enlève tout renseignement indiquant sa provenance électronique avant de l'acheminer à votre destinataire; et
 - les logiciels de protection de la mémoire, qui sont programmés pour empêcher tout accès en direct interdit à votre ordinateur. Certains de ces logiciels peuvent même tenir un journal de toute activité survenue à votre ordinateur.

Mais la nature de l'Internet est telle que les usagers doivent également se protéger avec leurs propres moyens. Voici donc certaines suggestions qui pourraient garantir votre vie privée dans l'univers électronique. Ces suggestions sont inspirées (avec la permission de sa directrice et tous nos remerciements) du *Privacy Rights Clearinghouse* du *Center for Public Interest Law* de l'Université de San Diego en Californie.

- **Dotez-vous d'un mot de passe inviolable** : votre mot de passe devrait être le plus absurde possible, combinant majuscules, minuscules, chiffres et symboles, et personne ne devrait pouvoir le deviner à partir d'un nom, d'un anniversaire ou d'un intérêt personnel;
- **Demandez à votre fournisseur de services informatiques une copie de sa politique de protection de la vie privée** : la plupart des fournisseurs commerciaux ont une telle politique, qu'ils communiquent généralement à leurs nouveaux abonnés. Ne vous abonnez pas aux fournisseurs qui n'en ont pas. Lisez attentivement tous les messages qui apparaissent à votre écran en début de session : beaucoup de fournisseurs inspectent vos messages électroniques et exigent cette capacité de leurs nouveaux abonnés;
- **Faites le tour** : apprenez-en le plus possible sur un nouveau service avant de l'utiliser. Affichez vos questions dans un groupe de discussion reconnu. Les autres usagers s'empresseront de vous mettre au courant de leurs mauvaises expériences, car ces nouvelles voyagent vite sur l'Internet;
- **Prenez pour acquis que vos communications ne resteront pas confidentielles** : à moins que vous ne chiffriez vos transmissions à des groupes de discussion, vos avis publics, vos messages électroniques ou votre notice biographique en direct, n'y incluez aucun renseignement personnel de nature délicate (numéro de téléphone, d'assurance sociale ou de carte de crédit, mot de passe, adresse, dates de vacances);
- **Méfiez-vous des logiciels de démarrage** : ces logiciels, programmés pour établir votre abonnement à un service quelconque, vous demandent quelquefois de leur fournir votre numéro d'assurance sociale, de carte de crédit ou de votre compte-chèque, lequel est automatiquement valide à des fins de facturation. Ces logiciels peuvent aussi quelquefois accéder à votre insu aux données contenues dans votre ordinateur. Demandez plutôt à votre fournisseur de services de vous abonner d'une façon différente;
- **Effacez vos traces de "pas"** : servez-vous d'entreprises d'acheminement anonyme de vos messages afin de ne pas laisser d'indication du début ni du contenu de vos sessions tant dans le serveur de votre fournisseur de services que dans des ordinateurs éloignés;

Internet et vie privée : guide de l'utilisateur

Il y aurait au dernier calcul (si peu précis soit-il) quelque 40 millions d'utilisateurs, commerciaux ou autres, de l'Internet de par le monde. Et il est surprenant de constater à quel point la plupart de ces gens ignorent que leurs communications, leurs transactions ou le contenu de leur ordinateur sont accessibles, à moins qu'ils ne l'empêchent consciemment, à qui le veut bien.

Cette exposition au sein de l'Internet ne devrait surprendre personne : à ses débuts comme réseau de communications du ministère américain de la Défense, l'ARPANET (son nom d'alors) relayait des bases militaires, des centres universitaires de recherche et des fabricants de matériel de défense. L'ARPANET devait rester ouvert et accessible afin de permettre la communication et de résister à toute attaque nucléaire, et d'autres réseaux informatiques et universités s'y sont progressivement greffés.

L'Internet d'aujourd'hui est un ensemble de réseaux dont les innombrables liens relient une multitude d'ordinateurs. Un message destiné à un correspondant de votre ville pourrait bien faire le tour du monde avant d'être livré à bon port, et chaque message suit rarement deux fois le même trajet. L'Internet est ici et nulle part tout à la fois : il n'a aucun siège social et personne n'en est responsable. C'est ce qui fait sa force... et ce qui menace notre vie privée.

Une fois assis tranquillement devant votre écran d'ordinateur, il est facile d'oublier qu'un message électronique, loin de ressembler à un appel téléphonique, équivaut plutôt à une annonce publique : vous ne devriez donc pas vous attendre à ce qu'il reste confidentiel. En fait, non seulement vos messages électroniques (y compris ceux destinés à des groupes de discussion publics ou spécialisés) sont-ils accessibles à quiconque, mais il existe également des logiciels sur l'Internet dont le rôle est de compiler un profil de vos messages et de vos intérêts. Et le moment n'est pas loin où les compagnies de marketing compileront systématiquement ces profils pour en tirer des listes uniques au moyen desquelles ils vous vendront électroniquement leurs produits ou leurs services. N'oublions pas non plus que les transactions commerciales ou bancaires conclues sur l'Internet comportent des risques, à moins qu'elles ne soient chiffrées.

La puissance et l'étendue de l'Internet permettent à ses usagers et aux gestionnaires de ses systèmes un accès illimité à quantité de renseignements personnels ou autres. Consciente de l'impact social que pouvait avoir la profession de ses membres, la *Association for Computing Machinery* s'est dotée en janvier 1989 d'un code d'éthique encadrant les responsabilités de ces derniers. L'une de ces responsabilités est le "respect de la vie privée d'autrui".

candidat. Puisque la Directive ministérielle de 1987 sur l'accès au casier judiciaire en est actuellement à être révisée, le moment semble bien choisi pour créer ce deuxième fichier.

La révocation d'une grâce La *Loi sur le casier judiciaire* donne à la Commission nationale des libérations conditionnelles le droit de révoquer la grâce accordée à un individu après que celui-ci ait pu lui présenter ses arguments.

Cette loi stipule également la révocation de la grâce lorsque l'individu est reconnu coupable d'un nouveau délit ou infraction : la loi exige alors de la GRC qu'elle reconstitue dans le système de gestion des casiers judiciaires toutes les accusations visées par la grâce. Puisque l'individu ne peut pas présenter ses arguments à l'effet contraire, ni même savoir que sa grâce a été révoquée, il pourrait ignorer que ces renseignements sont de nouveau disponibles et peuvent être utilisés à son encontre.

Dans un esprit de transparence, la GRC devrait incorporer à ses pratiques celle de prévenir, autant que possible, tout individu de la révocation de sa grâce.

La description du fichier Les casiers judiciaires de la GRC ne sont pas obligatoirement complets, puisque les corps policiers et agences correctionnelles ne sont pas tenus d'y verser leurs renseignements. La description actuelle du fichier dans *InfoSource* ne reflète pas cet état de fait et pourrait porter le lecteur à croire que ces casiers judiciaires sont complets. La GRC devrait par conséquent corriger cette description et la rendre plus exacte.

Veuillez nous contacter, soit directement ou par le biais de notre site Web, pour obtenir une copie de notre étude du système de gestion des casiers judiciaire de la GRC.

Le système de gestion des casiers judiciaires

Ce système, sous le contrôle de la Gendarmerie royale du Canada, est un outil essentiel pour les corps policiers et autres agences chargées d'enquêtes criminelles. Ce fichier de renseignements, intitulé "Casiers judiciaires, résumés de renseignements judiciaires et empreintes signalétiques", porte le numéro de référence PPU 030, et tombe sous le coup de la *Loi sur la protection des renseignements personnels*. Au cours de l'exercice financier qui vient de s'achever, le Commissariat s'est penché sur les composantes et la gestion de ce fichier.

Notre étude nous a permis de rectifier certaines perceptions erronées que nous avions du système, notamment au chapitre des renseignements qu'il contient et de la façon dont il est géré. La GRC est pleinement consciente de la nature délicate de ces renseignements, du besoin de s'assurer de leur exactitude, ainsi que de la responsabilité qui lui incombe de bien les gérer. Les entrevues que nous avons tenues avec des employés de la GRC et d'autres corps policiers nous ont confirmé tous les efforts que déploie la GRC afin de limiter l'accès à ces renseignements aux personnes et aux agences qui en ont un besoin réel.

Bien que la GRC gère généralement ce système conformément à la *Loi sur la protection des renseignements personnels*, nous avons cependant déterminé certains points sur lesquels la GRC pourrait davantage adhérer à cette dernière.

Le mandat Bien que notre étude ait relevé le nom de plusieurs lois faisant référence au rôle de gestionnaire du système qu'est la GRC, ni cette dernière ni le Commissariat n'ont pu établir l'existence d'un texte habilitant. Les renseignements contenus dans le système étant utilisés quotidiennement par des corps policiers et autres dans le cadre de décisions ayant un impact important sur des individus, il nous semble qu'une nouvelle loi habilitante ou, à défaut, des modifications à une loi existante répondrait mieux aux besoins de la GRC et de la population canadienne. Cette loi devrait clairement indiquer les renseignements pouvant être recueillis, les usages pouvant en être faits, ainsi que les personnes ou organismes pouvant y avoir accès.

Le contenu Un casier judiciaire renferme actuellement non seulement les accusations ayant mené à une condamnation, mais aussi celles ayant été retirées, ou pour lesquelles un jugement a été différé ou l'individu innocenté. Bien que ces trois dernières catégories d'accusation puissent présenter une certaine utilité pour les corps policiers, elles devraient être versées dans un fichier distinct auquel l'accès serait encore plus restreint. Ce second fichier ne serait accessible que dans le cadre de certaine enquêtes criminelles, et serait soustrait à la curiosité de tout un chacun, tel l'employeur vérifiant les antécédents d'un employé ou d'un

C'est inexact. La Loi sur la protection des renseignements personnels interdit effectivement la communication de renseignements personnels en général, mais le permet si un organisme fédéral détermine qu'il en serait clairement dans l'intérêt de la population. L'organisme doit d'abord prévenir le Commissaire à la vie privée de son intention de divulguer les renseignements. Nous étudions alors les circonstances entourant chaque cas, ainsi que les renseignements affectés. Puis, bien que le Commissaire ne puisse interdire la divulgation des renseignements, il peut en prévenir le criminel visé s'il le décide.

Assurons-nous tous de bien saisir la situation : le Commissaire à la vie privée ne dispose d'aucun pouvoir, si ce n'est dissuasif, d'empêcher la communication à la population de renseignements personnels au sujet d'un criminel considéré comme dangereux. Le Commissaire à la vie privée ne peut ni provoquer ni interdire une telle divulgation. Et en fait, la Loi sur la protection des renseignements personnels contient des dispositions facilitant la communication de renseignements

personnels au nom de l'intérêt du public.

Un équilibre précaire

Il n'existe pas de solution facile au problème de la protection de la société contre certains de ses membres. Nous recommandons cependant d'évaluer certains facteurs avant de conclure au bien-fondé de la divulgation de renseignements personnels. Se retrouvent au nombre de ces facteurs les risques de récidive du criminel, l'efficacité de mesures autres que la divulgation des renseignements, les impacts de cette divulgation tant pour la population que pour le criminel, et l'ampleur du battage publicitaire requis.

Les programmes en vigueur au Manitoba et en Colombie-Britannique semblent représenter un juste milieu entre le besoin de la population de connaître la présence d'une personne potentiellement dangereuse et le droit à la vie privée de cette dernière. Le document que nous avons préparé appuie sous réserve de tels programmes, à condition qu'ils s'appliquent à n'importe quel criminel considéré dangereux, et non simplement aux criminels sexuels. Celles des provinces ne disposant d'aucun programme de ce genre pourraient recourir aux services d'un comité de citoyens nommés par le gouvernement fédéral, lesquels étudieraient chaque cas de divulgation de renseignements au nom de l'intérêt public et soumettraient leurs recommandations à Service correctionnel Canada, la GRC et la Commission nationale des libérations conditionnelles.

Veuillez nous contacter, soit directement ou par le biais de notre site Web, pour obtenir une copie de notre document.

la communication par le gouvernement de renseignements personnels reliés à ces derniers. Et ce sont de telles divulgations qui ont attiré le Commissaire à la vie privée du Canada et ses homologues provinciaux dans le débat.

Dans certains cas, il est possible d'empêcher un criminel de récidiver par le simple fait de prévenir la population locale de sa présence. Dans d'autres cas, cependant, de telles annonces peuvent avoir des conséquences bien plus graves :

- certains criminels pourraient tenter de se soustraire à la publicité qu'ils causent en se cachant et en refusant tout traitement, devenant de la sorte encore plus dangereux;
- la population locale peut croire, mais à tort, qu'elle connaît tous les criminels dangereux, alors qu'en fait beaucoup restent inconnus;
- le battage publicitaire qui entoure la remise en liberté d'un criminel peut empêcher la réintégration de ce dernier dans une société qui ne veut pas de lui et le chasse;
- la divulgation de renseignements personnels au sujet de criminels dangereux peut, beaucoup d'entre eux ne récidivant pas, leur causer des torts injustifiés;
- l'annonce de la présence de certains criminels peut mener à des agressions sur leur personne, sans pour autant s'avérer bénéfique pour la société.

De notre point de vue, toute mesure affectant la vie privée d'un criminel doit profiter à la société. La communication de renseignements personnels devrait être interdite lorsqu'il n'en résulte pas de bénéfices. Et deux questions restent en suspens : à quel moment est-il préférable de divulguer les renseignements personnels d'un criminel remis en liberté, que ce soit sous conditions, après avoir purgé sa peine ou que cette dernière ait été remise? Et qui devrait avoir le droit de communiquer les renseignements, et à qui?

Le document du Commissariat présente plusieurs scénarios de communication, dont ceux du Manitoba et de la Colombie-Britannique, en ce qui a trait à la remise en liberté de criminels dangereux. Dans ces deux provinces, les principaux intérêts (corps policiers, services correctionnels et, au Manitoba, groupes de pression) se penchent sur le cas de chaque criminel et décident alors de la nécessité ou non d'en divulguer des renseignements personnels, et à quel point.

La Loi au banc des accusés

Les responsables sont souvent nombreux à prétendre que la *Loi sur la protection des renseignements personnels* les empêche de communiquer tout renseignement permettant d'identifier un pédophile ou autre criminel dangereux au sein de la population, et ce même s'il y avait intérêt à le faire.

Silence ou publicité?

La population semble de plus en plus opposée à la remise en liberté, sous conditions ou en fin de peine, de criminels jugés dangereux, surtout des pédophiles. Cela comporte des risques, en effet, que les Canadiens ont le droit d'essayer de réduire. L'incident de Fort St-John en Colombie-Britannique illustre bien le cas.

Avertis de la présence au sein de leur communauté d'un criminel sexuel bien connu, les membres du conseil municipal de Fort St-John ont appuyé certains groupes locaux de pression qui ont imprimé et distribué des affiches révélant la présence de l'individu. Ensuite, les membres du conseil ont voté la communication de ces renseignements à d'autres localités de leur province, du Yukon et de l'Alberta. Les affiches contenaient la photo de l'individu, sa description, la liste de ses condamnations et une mention des accusations qui avaient été retirées.

Le Commissaire à la vie privée du Canada et son homologue provincial de la Colombie-Britannique, monsieur David Flaherty, se sont penchés sur cet incident. Le docteur Flaherty s'est concentré sur les gestes posés par les membres du Conseil, alors que nous avons étudié l'allégation que la Gendarmerie royale du Canada avait communiqué à tort des renseignements au maire de Fort St-John (bien qu'ils semblent avoir été de nature publique). Les deux commissaires en ont conclu que l'approche "mitrailleuse" (telle que décrite par M. Flaherty) était rarement appropriée, quoique la communication de renseignements puisse être quelquefois justifiée. Les deux commissaires pensent qu'une politique nationale et un processus uniformes aideraient à décider de chaque communication.

Afin de faire un peu la lumière sur ce sujet hautement controversé, le Commissariat a publié un document à des fins de discussions intitulé

L'identification des criminels dangereux remis en liberté.

Le rôle de protéger le public de criminels dangereux revient principalement aux tribunaux, aux établissements de soins psychiatriques et aux organismes d'aide sociale. Mais les tribunaux ne sont pas infaillobles, et les programmes de réhabilitation dispensés par les pénitenciers ne sont pas toujours efficaces. Les gouvernements et la population cherchent alors d'autres méthodes de protection.

La publicité serait-elle la solution?

Le barrage publicitaire devient la solution bon marché d'un problème autrement complexe découlant en partie des faiblesses inhérentes au système correctionnel. Mais cette initiative implique également, et ce sans le consentement des criminels,

Le CRTC, reconnaissant le droit de la White Directory de faire concurrence aux compagnies telles que Télédirect, a cependant ordonné aux grandes entreprises téléphoniques de permettre à leurs clients de faire retirer leurs noms et adresses des fichiers électroniques qu'elles transmettaient à la White Directory. Cette dernière s'est opposée à ce mécanisme de retrait, dont elle disait qu'il ne lui permettrait pas de publier des annuaires aussi complets que ceux des grandes compagnies. Le CRTC a cependant maintenu sa décision, et la White Directory en a appelé auprès du Gouverneur en Conseil.

Le Commissaire à la vie privée appuie la décision du CRTC, et a écrit au Gouverneur en Conseil pour l'inciter à préserver le droit de chacun de pleinement contrôler ses renseignements personnels. Le Gouverneur en Conseil a un an pour rendre sa décision.

Industrie Canada envisage heureusement de limiter l'utilisation de balayeurs d'ondes capables de capter les communications numériques. L'on devrait cependant aller plus loin et interdire aux compagnies fournissant des SCP d'utiliser ou de communiquer tout renseignement relié à l'emplacement de l'utilisateur, sauf évidemment pour lui transmettre ou facturer une communication. De plus, les factures de SCP ne devraient pas indiquer l'emplacement exact de l'un ou l'autre des interlocuteurs.

Quoque le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) ne réglemente pas les fournisseurs de SCP, ses membres tiendront plus tard cette année des audiences publiques afin de déterminer quels aspects des communications sans fil (dont les SCP) devraient être du ressort du CRTC. Si le gouvernement et les fournisseurs réussissent à protéger les combinés, les communications et les renseignements de localisation des SCP, cette nouvelle technologie pourra pleinement profiter aux Canadiens au lieu de les assujettir à une nouvelle forme de surveillance.

Autres nouvelles dans le domaine

La déréglementation du service téléphonique au Canada a fait surgir plusieurs problèmes, dont certains découlent du droit des compagnies rivales d'avoir accès à la liste des clients des grandes compagnies téléphoniques. Cet accès a eu comme conséquence immédiate une avalanche d'appels téléphoniques et de prospectus publicitaires, et certains clients se sont retrouvés inscrits auprès d'une nouvelle compagnie de service interurbain sans y avoir consenti, ni même l'avoir su avant d'en recevoir leur première facture!

Le CRTC autorise effectivement les grandes entreprises téléphoniques à communiquer sur demande à ces nouvelles compagnies les coordonnées d'un usager si ce dernier y consent. Mais ces nouvelles compagnies (qui achètent des blocs d'appels interurbains des grandes entreprises et les revendent aux clients) ne relèvent pas de la juridiction du CRTC. Cependant, les clients qui le désirent peuvent être rebranchés sans frais à leur première compagnie.

Sur un autre front, les éditeurs privés d'annuaires téléphoniques continuent leur récente poussée pour obtenir accès aux bases de données informatiques des clients des grandes compagnies téléphoniques. Cet accès leur permettrait de publier des annuaires concurrents. Il y a deux ans, la compagnie White Directory of Canada a demandé au CRTC d'autoriser un tel accès, visant surtout les bases de données publiées par une filiale de Bell Canada, Télé-Direct.

Parlons de télécommunications

Nous sommes tous d'accord pour dire que la technologie améliore quelquefois (mais pas toujours) notre qualité de vie, mais qu'elle peut porter atteinte à notre vie privée. Ses créateurs ne comprennent pas toujours tout son potentiel, et ses usagers encore moins. Le respect de la vie privée est quelquefois la victime de l'esprit d'entreprise, comme l'illustreront, cette année encore, les exemples suivants.

Services de communications personnels (SCP)

En décembre 1995, Industrie Canada émettait des permis à quatre compagnies, les autorisant à élaborer et vendre des SCP. Ces petits appareils qui tiennent dans la main permettent la transmission de la voix, de texte, de graphiques et d'images vidéo par le biais d'un combiné se rapprochant d'un téléphone cellulaire. Ils diffèrent cependant de la technologie cellulaire en ce qu'ils ne fonctionnent pas sur les mêmes fréquences, et que leurs transmissions sont numériques, et non analogiques. La numérisation des communications les rend moins chères et en accroît la qualité (notamment quant au texte et aux images) et la sécurité.

Mais quel est donc le problème, puisque les SCP semblent nettement supérieurs aux communications cellulaires? Il y a en fait deux problèmes, dont les Canadiens devraient être au courant.

Le premier tient au fait que les SCP transmettent leurs communications sur les ondes publiques. Ces communications peuvent donc être interceptées tout comme les communications cellulaires, même si cela exige un matériel plus dispendieux et sophistiqué. Le second problème découle de la nature même des SCP : votre emplacement exact doit être connu en tout temps pour qu'une communication vous parvienne : chez vous, sur la pente de ski ou dans un centre d'achats. Et si cela vous dérange, imaginez un peu l'intérêt qu'aurait un criminel, un conjoint jaloux ou un vendeur quelconque à vous retrouver n'importe quand, n'importe où...

Il y a des solutions à ces deux problèmes :

- les communications pourraient être chiffrées, ce qui rassurerait la majorité des utilisateurs. Il est cependant possible quelquefois de décoder une communication chiffrée, ainsi que le prouvent les récentes troupes faites dans l'algorithme du fureteur Internet Netscape;
- le combiné pourrait être construit de telle sorte que son utilisateur légitime soit obligé d'en déverrouiller l'accès au moyen d'un code personnel.

Bien que le Commissariat appuie les efforts que déploie le gouvernement fédéral en vue d'un meilleur rendement, il n'en reste pas moins que l'intégration horizontale et la prestation commune de services peuvent porter atteinte à notre vie privée. Et même si nos consultations avec C&IC et DRHC ont quelque peu apaisé nos craintes, nul ne peut nier le risque que les projets découlant du *Plan directeur* peuvent effectivement mener à la création, pour chaque individu, d'un dossier informatisé unique auquel accéderait tout organisme fédéral, provincial, privé ou étranger qui en aurait besoin.

Ce scénario est non seulement incompatible avec le libellé actuel de la *Loi sur la protection des renseignements personnels*, il réveille également le spectre d'une société de surveillance, au sein de laquelle chacun pourra tout savoir sur autrui. N'oublions jamais les deux vérités suivantes : aucun réseau d'ordinateur de par le monde n'a encore pu résister à un pirate informatique, et l'utilisateur est le plus grand danger qui menace la sécurité des renseignements contenus dans un ordinateur.

Les progrès de la technologie réduisent notre capacité de contrôler nos renseignements personnels. Ces progrès peuvent même diminuer l'efficacité des lois protégeant notre vie privée, cette dernière devenant d'autant plus difficile à sauvegarder que les systèmes informatiques croissent en complexité et en grandeur.

Mais il ne faut pas pour autant abandonner la lutte, ni accepter ces commentaires négatifs voulant que le respect de la vie privée soit un obstacle à la conception de nouveaux systèmes informatiques. Cette accusation trop souvent entendue n'est en fait qu'une piètre excuse visant à faire porter par autrui la responsabilité d'un oubli en début de processus.

Cette accusation est fautive et révèle un manque de vision. Le respect de la vie privée, loin d'être un obstacle à la conception d'un bon système informatique, en est au contraire un élément essentiel, ainsi que de la gestion de tout renseignement. Le respect de la vie privée permet à la population de faire confiance aux systèmes informatiques du gouvernement fédéral.

Prestation commune de services

La seconde tendance que suivent les ministères fédéraux et qui comporte des risques quant au respect de la vie privée est la prestation de services conjointement avec d'autres organismes fédéraux ou paliers de gouvernement, ou même avec le secteur privé. Les citoyens ne peuvent qu'applaudir ce concept, qui leur permet de n'aller qu'à un seul endroit pour payer leurs impôts municipaux, renouveler leur permis de conduire, réclamer leurs prestations d'assurance-emploi ou demander un prêt étudiant. Les risques pour la vie privée sont cependant évidents : comment assurer une protection efficace des renseignements lorsque plusieurs paliers de gouvernement y ont accès? Les données seront-elles entreposées au même endroit que les terminaux d'accès? Vos renseignements relèveront-ils du "contrôle" du gouvernement fédéral ou seront-ils assujettis aux lois provinciales de protection de la vie privée? Si le centre de prestation de services est géré par une entreprise privée, le contrat liant cette dernière comportera-t-il des dispositions l'obligeant à protéger vos renseignements, ou ces derniers resteront-ils sans protection?

La prestation commune de services doit être assurée avec le plus grand soin, au même titre que l'entrepasage de données. Tout partenariat avec les gouvernements provinciaux ou municipaux doit être précédé d'une connaissance claire et sans équivoque des obligations de chaque partenaire. Et la solution n'est pas l'adoption du plus faible niveau de protection de la vie privée, car cette protection est quasi inexistante dans certaines juridictions.

L'entreposage de données

Cette activité constitue peut-être la démarche la plus significative entreprise par le gouvernement fédéral pour la gestion des renseignements qu'il détient. Un nombre croissant d'organismes fédéraux "construisent" des "entrepôts" dans lesquels ils placent et manipulent l'ensemble des données reliées à leurs activités, y compris les renseignements personnels en fonction desquels ils décident du sort de certains individus. DRHC et Anciens combattants Canada ne sont que deux des ministères mettant sur pied de tels "entrepôts".

En termes plus pratiques, ces derniers sont en fait de gigantesques bases de données qui intègrent des renseignements en provenance de diverses sources, en rectifient les erreurs, puis les entreposent de sorte à en faciliter la recherche, l'analyse et le traitement. Il ne s'agit plus de séparer les renseignements en fonction de leur utilisation (p.e. le paiement d'impôts, une demande de prêt étudiant ou l'accès aux prestations du Régime de pensions du Canada), mais plutôt de regrouper tous les renseignements reliés à une personne donnée et de les cataloguer sous son nom et autres éléments identificateurs. Pour prendre connaissance de toutes les transactions que cette personne a effectuées avec le gouvernement fédéral, il ne reste plus qu'à la retrouver dans "l'entrepôt".

Les responsables fédéraux en sont très heureux. Mais l'horizon est autrement plus sombre pour ce qui est de notre vie privée. Puisque ces "entrepôts" de données visent à centraliser les renseignements fédéraux, ils offrent de ce fait davantage à la curiosité des gens, et certains renseignements risquent d'être utilisés à des fins bien différentes de celles pour lesquelles ils avaient été recueillis. De plus, cette centralisation de renseignements provoque inévitablement une demande accrue, et insatiable, d'information tirée de ces derniers. Ce danger est bien connu du milieu des défenseurs de la vie privée. Il faut rajouter à cela la possibilité qu'offrent ces "entrepôts" d'élaborer des profils détaillés des personnes qui y sont fichées, ou pire encore, de pénétrer dans l'intimité de ces personnes en analysant les détails de leurs transactions avec le gouvernement.

En bout de ligne, ces "entrepôts" exigeront la création d'un numéro d'identification unique permettant l'accès au dossier de chaque individu. Ah! ce numéro unique, ce dossier unique, cette unique carte d'identité sans laquelle nous ne sommes rien ni personne... Comme dans tout système informatique moins sophistiqué, la supprime importance de nos renseignements personnels risquera d'éclipser notre propre existence, nous ravalant au simple rang de "0" et de "1" dans un quelconque "entrepôt".

Le grand partage

Le Secrétaire du Conseil du Trésor a publié au début de 1994 un *Plan directeur pour le renouvellement des services gouvernementaux à l'aide des technologies de l'information* en réponse aux attentes du gouvernement fédéral, lequel voulait une fonction publique réduite et plus efficace. Ce *Plan directeur* encourage chaque organisme fédéral à recourir à l'informatique pour simplifier ses activités et éliminer tout processus inefficace.

Puisque plusieurs des recommandations du *Plan directeur* affectent la façon dont le gouvernement fédéral gère les renseignements personnels dont il a le contrôle, le Commissariat s'est dit intéressé à être impliqué dans les projets découlant du *Plan directeur*. Des quelque 30 organismes fédéraux s'étant depuis penchés sur leurs activités, deux se démarquent particulièrement, et nous ont invités à les conseiller.

Citoyenneté et Immigration Canada (C&IC) a entrepris le premier projet d'envergure découlant du *Plan directeur* : la refonte de l'ensemble de ses processus d'affaires suscite l'intérêt d'autres ministères, lesquels y voient un projet d'essai. C&IC vise une "intégration horizontale" de ses activités, ce qui signifie un partage accru, tant au sein du ministère qu'avec d'autres organismes, de renseignements reliés aux immigrants et demandeurs du statut de réfugié. À l'heure actuelle, ces renseignements sont cantonnés aux programmes qu'ils concernent, un schéma "vertical" de l'information commun à l'ensemble de la fonction publique fédérale. Une fois la refonte de ses processus d'affaires terminée et ces derniers devenus "horizontaux", C&IC aura intégré tous les renseignements dont il a le contrôle.

Développement des ressources humaines Canada (DRHC) est l'autre chef de file en matière de projets découlant du *Plan directeur*. Ce ministère est en train de simplifier la gestion de ses programmes d'assurance-emploi, du Régime de pensions du Canada, de la formation de la main-d'oeuvre et des banques d'emploi, éliminant ainsi bon nombre de ses Centres d'emploi du Canada. DRHC desservira plusieurs localités par le biais de kiosques électroniques ou de centres satellites ou téléphoniques, et s'associera dans de nombreux cas à des entreprises du secteur privé, des sociétés de la Couronne, des agences spéciales ou même des gouvernements provinciaux et municipaux.

Ces deux ministères illustrent bien deux des tendances que suit le gouvernement fédéral, lesquelles comportent des risques si elles ne sont pas bien étudiées. Ces deux tendances sont l'entrepassement de données et la prestation commune de services.

- la loi devrait interdire la communication de renseignements tirés de la liste électorale, à moins que cette communication ne se fasse à des fins d'élections qu'aux provinces, municipalités ou conseils scolaires capables d'en assurer une protection égale à celle du gouvernement fédéral.
 - les renseignements de la liste électorale ne devraient servir qu'à l'exercice du droit de vote des personnes qui y sont inscrites;
 - ces renseignements ne devraient être recueillis qu'après et au su des personnes concernées, et ce avec leur consentement;
 - il ne faudrait recueillir des personnes qui le souhaitent que les renseignements personnels nécessaires à l'exercice de leur droit de vote;
 - la population se rend à la nécessité d'une liste électorale permanente, une telle liste ne devrait voir le jour qu'aux conditions suivantes :
- La meilleure façon de protéger notre droit à la vie privée est de résister à la tentation de gérer un programme gouvernemental par le biais de la collecte et de l'information d'une grande quantité de renseignements personnels. S'il est impossible de concevoir un processus électoral sans effectuer une telle collecte, et si la population se rend à la nécessité d'une liste électorale permanente, une telle liste ne devrait voir le jour qu'aux conditions suivantes :

Ce qu'il faut faire

Le DGE nous a laissé savoir que toute demande d'accès à la liste électorale pour des fins autres que celles de sa création (auxquelles s'opposerait farouchement le Commissaire) devrait être sanctionnée par le Parlement après avoir l'objet d'un débat public.

Usages secondaires de la liste La plus grande préoccupation du Commissaire reste les usages secondaires qui pourraient découler d'une liste de la majorité des électeurs, laquelle liste serait d'un énorme intérêt pour bien des organismes publics. Les autres paliers de gouvernement ayant informatisé leur liste électorale ont rapidement dû y permettre l'accès à leurs divers organismes, car il est difficile de résister à de telles demandes. Il n'y a qu'à constater l'accès croissant aux fichiers de l'impôt (lesquels étaient quasi intouchables il n'y a pas si longtemps) pour en déduire que la liste électorale connaîtrait un sort semblable.

renvoys directement au DGE. Ce dernier a accepté de se pencher sur cette suggestion.

renseignements au DGE. Ce système est déjà en vigueur en Colombie-Britannique. Le DGE pourrait aussi créer un formulaire distinct lequel accompagnerait tout courrier en provenance du gouvernement fédéral et serait

Ce que nous en pensons

Le recensement visant à recueillir directement auprès de chacun les renseignements le concernant est une initiative louable et compatible avec la *Loi sur la protection des renseignements personnels*. Chaque personne pourra alors décider si elle souhaite être inscrite ou non à cette liste. Cependant cela soulève plusieurs inquiétudes.

Numéro de téléphone Le Commissariat a remis en question la suggestion d'ajouter le numéro de téléphone aux renseignements contenus dans les listes électorales traditionnelles. Le numéro de téléphone n'est pas actuellement nécessaire et son apparition sur une liste électorale pourrait susciter des appels importuns. Le DGE nous a répondu que ce numéro ne servirait qu'à des fins internes et n'apparaîtrait pas sur la liste.

Collecte de renseignements supplémentaires Nous étions également préoccupés des dispositions qui permettraient au DGE de recueillir de plus amples renseignements, ouvrant ainsi la porte à la possibilité d'une collecte excessive de renseignements personnels que le législateur n'aurait pas prévue. Ces dispositions visent en fait à permettre au DGE de recueillir tout renseignement supplémentaire exigé par une loi électorale provinciale, une clarification que le DGE s'est engagé à préciser dans son projet de loi.

Communication annuelle aux députés Il nous a semblé exagéré de vouloir communiquer annuellement à chaque député la liste des électeurs de sa circonscription. En effet, la liste électorale ne doit officiellement servir qu'à la tenue d'élections ou de référendums. Or puisque personne ne tient d'élections chaque année, une telle communication semble davantage permettre aux partis politiques de se livrer à de la prospection. Le DGE a accepté de revoir la pertinence de cette disposition.

Collecte par couplages de données La tenue à jour de la liste par le biais de couplages avec d'autres fichiers ou registres fédéraux est préoccupante. Le Commissaire s'oppose en principe à toute exploration de bases fédérales de données pour des raisons autres que celles justifiant l'existence de ces dernières. Le couplage de données est une pratique invisible qui ne respecte pas les exigences de la *Loi sur la protection des renseignements personnels*. Il serait préférable que les renseignements recherchés soient recueillis directement auprès des Canadiens, à leur su et avec leur consentement.

Le Commissaire a suggéré d'incorporer une case de consentement aux formulaires d'autres organismes fédéraux, laquelle permettrait par exemple à Revenu Canada ou à Développement des ressources humaines Canada de faire suivre les

Les changements que vient de proposer le Directeur général des élections (DGE) du Canada à la *Loi électorale du Canada* lui donneraient, une fois adoptés, le pouvoir de constituer une liste électorale permanente. La notion d'une telle liste remonte à 1991, alors qu'une Commission royale sur la réforme électorale s'y était attardée, sans pour autant la recommander au gouvernement. Les Canadiens se sont toujours opposés à ce type de liste, car tout registre de la population constitue une réelle menace aux droits et libertés individuels : certains soutiendraient que le temps de la guerre, en effet, sont gravés dans l'esprit de nombreuses personnes.

Les élus changent, cependant. En cette époque de "responsabilité fiscale", la possibilité de réduire les dépenses publiques de millions de dollars rend appréciable ce qui, hier encore, était inacceptable. Impératifs budgétaires et efficacité accrue, voilà les deux raisons invoquées par la Colombie-Britannique et le Québec lors de leur récente mise sur pied d'une liste électorale permanente. Au tour maintenant du gouvernement fédéral. Mais les impératifs précédents ne doivent pas faire oublier d'autres considérations tout aussi importantes.

Ce qui est proposé

Il s'agirait d'établir la liste permanente au moyen d'un dernier recensement conventionnel de la population. Les recenseurs recueilleraient de chaque électeur son nom, son adresse, son sexe, sa date de naissance, son numéro de téléphone et une preuve de sa citoyenneté canadienne. La population pourrait devoir fournir de plus amples renseignements si le DGE l'estimait nécessaire. Une fois recueillis, les renseignements seraient validés et versés dans une base de données informatisée. Personne ne serait obligé de s'inscrire, et chacun pourrait en tout temps faire enlever son nom de la liste.

À intervalles réguliers, le DGE comparerait la liste aux fichiers de l'impôt et des permis de conduire (pour mettre les adresses à jour), aux registres d'état civil (pour enlever les noms des personnes décédées), aux dossiers de citoyenneté (pour rajouter les noms des personnes naturalisées aptes à voter), ainsi qu'aux listes post-électorales provinciales (pour obtenir les plus récents renseignements). Les provinces, municipalités et conseils scolaires auraient accès aux données de la liste sur demande à des fins électorales. Chaque député recevrait annuellement les renseignements de la liste ayant trait aux électeurs de sa circonscription.

- la loi établissant la base de données devrait comporter un mécanisme complet de révision, incluant une vérification de conformité, d'ici deux ou trois ans après l'entrée en vigueur de la loi.

Cette vérification de conformité est d'une réelle importance : deux ou trois ans d'utilisation devraient suffire à déterminer l'utilité de la base de données pour la résolution de crimes, et à nous assurer qu'elle ne servira à aucun usage imprévu. Il faut éviter que ne s'allonge la liste des crimes requérant une base de données ou le prélèvement d'échantillons génétiques. Nombreux sont ceux qui le réclament déjà, réagissant ainsi à l'existence même de la technologie et de la croyance que cette dernière peut résoudre tous nos problèmes si nous le lui permettons.

Aucun projet de loi traitant des éléments laissés pour compte dans l'analyse médico-légale des échantillons génétiques n'a encore été soumis au Parlement. Ce projet de loi sera soigneusement scruté afin de nous assurer qu'il satisfait bien à nos critères.

En terminant, nous tenons à féliciter tant le ministère de la Justice que celui du Solliciteur général d'avoir reconnu que le respect de la vie privée était au nombre des questions les plus importantes soulevées par le prélèvement d'échantillons de la création de bases de données génétiques. Nous les remercions également de nous avoir impliqués *avant* que la loi ne soit concrétisée. Leur volonté de nous consulter a permis que soient débattues les préoccupations reliées à la vie privée avant qu'il ne soit trop tard et qu'un changement ne crée d'embarras politique.

Naissance d'une base de données génétiques

Dans notre rapport annuel de l'année précédente, nous annonçons que le Parlement était sur le point d'adopter une loi autorisant les corps policiers à se procurer des échantillons génétiques auprès d'un individu soupçonné d'un crime grave. Cette loi a été promulguée en juillet 1995.

La loi ne traitait cependant pas de plusieurs points importants concernant la vie privée, notamment la possibilité de constituer une base de données d'échantillons génétiques ni les analyses tirées de ces spécimens. Au début de 1996, le Solliciteur général du Canada a publié un document de consultation intitulé *Une base nationale de données génétiques* qui soulevait plusieurs de ces questions toujours en suspens. Nous avons répondu à ce document en formulant diverses propositions, dont les suivantes :

- les échantillons ne devraient être prélevés à l'intention de la base de données (plutôt que dans le cadre d'une enquête prouvant le crime en question) qu'après la condamnation de la personne. Dans les cas moins graves, un mandat serait nécessaire pour l'obtention de l'échantillon, alors qu'elle se ferait automatiquement dans les cas plus sérieux;
- une fois l'analyse de l'échantillon inscrite dans la base de données, soit automatiquement ou suite à l'autorisation d'un juge, la police devrait pouvoir y accéder afin de comparer aux preuves prélevées sur les lieux d'un crime;
- seule l'analyse, et non l'échantillon, devrait être conservée dans le cas d'un inculpé. La destruction de l'échantillon préviendrait des utilisations ultérieures et réglerait la problématique éthique de la recherche de prédispositions génétiques au crime;
- l'utilisation d'un échantillon obtenu volontairement lors d'une enquête criminelle (lorsque la police, par exemple, demande à la population de lui remettre des échantillons génétiques afin de faciliter la recherche d'un criminel dangereux) devrait être limitée à l'enquête du crime visé. Les échantillons et leur analyse devraient être détruits dès la discussion des donneurs;
- les éléments identificatoires génétiques contenus dans la base de données ne devraient pas être conservés indéfiniment et devraient être détruits lorsqu'ils ne sont plus nécessaires (tel après le décès du criminel ou s'il s'est écoulé suffisamment de temps, des décennies dans certains cas, et que les risques de récidive sont pratiquement nuls);

renseignement contenu dans la puce. L'émetteur de la carte doit reconnaître le droit du détenteur d'exiger de tout organisme inscrivant des renseignements dans la puce de sa carte qu'il efface certains de ces renseignements.

Renseignements visibles sur la carte : les deux côtés de la carte ne devraient afficher que le minimum de renseignements personnels requis pour participer à un programme.

Le détenteur aura-t-il le droit d'accéder aux renseignements contenus dans la puce de la carte?

La Loi sur la protection des renseignements personnels reconnaît à chacun le droit de prendre connaissance des renseignements qui le concernent.

Nature des renseignements : le détenteur devrait pouvoir connaître la nature des renseignements contenus dans la puce.

Accessibilité des renseignements : le gouvernement devrait s'assurer que le détenteur dispose des moyens techniques pour prendre connaissance des renseignements contenus dans la puce de sa carte. Le gouvernement devrait également pouvoir expliquer ces renseignements au détenteur sur demande.

Journal : l'émetteur et les usagers de la carte devraient tenir un journal de toute nouvelle inscription de renseignements dans la puce de la carte, ainsi que de toute communication entre eux de renseignements reliés au détenteur. Ce dernier devrait pouvoir consulter ce journal.

Ce cadre de référence s'inspire de la liste de contrôle visant les nouvelles technologies publiée (en page 16) dans notre Rapport annuel 1992-93.

Pour obtenir le texte intégral de ce cadre de référence ou pour nous faire part de vos commentaires, veuillez vous adresser à nos bureaux soit directement ou par le biais de notre site Web.

destruction de la carte serait accompagnée de la dépersonnalisation de tous les renseignements reliés à son émission et à son contenu.

Comment les renseignements seront-ils utilisés et communiqués?
La Loi sur la protection des renseignements personnels comporte des principes de gestion équitable de l'information, déterminant notamment l'usage et la communication des renseignements personnels.

Lecture de la carte : le gouvernement devrait établir qui sera autorisé à lire le contenu de la carte, à quel point ce contenu sera accessible (en tout ou en partie), ainsi que les protocoles informatiques en permettant la lecture.

Restrictions à l'accès ou l'usage à des fins secondaires : le gouvernement devrait imposer des paramètres visant à interdire l'accès aux données contenues dans la carte, ou leur usage, à des fins autres que celles d'origine. Les données ne devraient être accessibles qu'aux personnes en ayant un besoin reconnu par la Loi sur la protection des renseignements personnels.

Restrictions à l'usage, la communication ou la copie à des fins interdites : le gouvernement devrait établir des balises afin d'empêcher les usagers de la carte d'en copier les renseignements de la puce vers une autre base de données pour s'en servir à des fins inconnues du détenteur.

Tous les usagers ou lecteurs de la carte à l'extérieur du gouvernement devraient se plier aux règlements contractuels stipulés par le responsable du programme gouvernemental, ne pouvant ainsi copier aucun renseignement contenu dans la carte sans l'autorisation préalable du détenteur.

Structure de la carte : la puce de la carte devrait compartimenter les renseignements qu'elle contient, tant pour en limiter quantitativement l'accès que pour clairement isoler les données d'identification, celles du programme et celles de nature délicate tels les renseignements médicaux ou d'urgence. Le gouvernement devrait séparer les applications à usages multiples afin d'éviter la fusion ou le débordement de certains renseignements. Les lecteurs et les appareils utilisés par les fournisseurs de services devraient chiffrer toute communication de données entre la puce de la carte et l'ordinateur central.

Le détenteur doit autoriser la lecture : aucun tiers ne devrait pouvoir accéder au contenu de la puce sans l'autorisation du détenteur (ou de son représentant en cas d'urgence). Cette autorisation pourrait être donnée par la composition d'un numéro d'identification personnelle ou d'un autre code.

Inscription de renseignements dans la puce, ou leur destruction : le gouvernement devrait indiquer les personnes autorisées à inscrire, modifier ou effacer, directement ou par le biais du fournisseur de services, tout

fonctionnement du système, les renseignements contenus dans la puce de la carte, et les personnes autorisées à les consulter ou à les modifier.

Le gouvernement devrait aussi aviser chaque détenteur de toutes les communications pouvant survenir entre l'organisme fédéral ayant émis la carte et les usagers de cette dernière (soient ceux fournissant les services reliés au programme).

Combien de temps l'organisme fédéral conservera-t-il les renseignements?

La Loi sur la protection des renseignements personnels requiert du gouvernement fédéral qu'il établisse des calendriers de conservation des renseignements personnels qu'il détient.

Conservation des renseignements : l'organisme émetteur et les usagers de la carte doivent planifier la conservation et l'élimination des renseignements. L'organisme émetteur devrait de plus instaurer un règlement régissant la nature des renseignements à conserver ainsi que les dispositifs de sécurité assurant leur confidentialité.

Comment l'organisme fédéral s'assurera-t-il de l'exactitude des renseignements qu'il détient?

La Loi sur la protection des renseignements personnels oblige un organisme fédéral à s'assurer de toutes les façons raisonnables que les renseignements personnels qu'il détient sont aussi exacts, à jour, et complets que possible.

Responsabilité d'un renseignement inexact : les usagers de la carte ne devraient pas automatiquement croire que les renseignements sont exacts du simple fait qu'ils sont contenus dans la puce de la carte : ces renseignements pourraient en fait être erronés, incomplets ou périmés. Il appartient autant à l'utilisateur qu'à l'organisme émetteur et au détenteur de la carte de s'assurer de l'exactitude des renseignements qu'elle contient.

Comment les renseignements seront-ils éliminés?

La Loi sur la protection des renseignements personnels oblige un organisme fédéral à contrôler l'élimination d'un renseignement personnel afin d'en interdire tout accès ultérieur ou toute communication défendue.

Renouvellement de la carte : le gouvernement devrait déterminer quels renseignements contenus dans la puce de la vieille carte devraient être reportés dans la nouvelle et si les vieux renseignements devraient être dépersonnalisés et soumis à des fins de recherche.

Destruction de la carte : un détenteur devrait pouvoir demander que sa carte soit détruite si cela est conforme au texte réglementant un tel acte. La

d'en garantir la confidentialité. Après tout, devons-nous nous adapter à la technologie, ou l'inverse? À nous de décider.

Cadre de protection pour les cartes à puce

La Loi sur la protection des renseignements personnels stipule la façon dont le gouvernement fédéral doit recueillir, utiliser, communiquer et protéger les renseignements personnels de ses clients et de ses employés. La Loi confie également à un commissaire indépendant le mandat d'en surveiller l'observation par les organismes fédéraux. Puisque les cartes à puce peuvent devenir d'importants instruments de collecte, d'entreposage et de communication de données, le Commissariat propose ici un cadre de référence qui permettra au gouvernement fédéral de respecter la vie privée des gens (ainsi que d'autres principes d'éthique) dès la conception des programmes faisant usage de cartes à puce. Les commentaires et suggestions de nos lecteurs sont les bienvenus.

La collecte des renseignements sera-t-elle nécessaire à un programme gouvernemental?

La Loi sur la protection des renseignements personnels exige qu'un organisme fédéral ne recueille de renseignements personnels que si ces derniers se rapportent directement à l'un de ses programmes ou à l'une de ses activités.

Cadre de référence juridique ou réglementaire : il existe un lien direct avec un programme ou une activité lorsqu'un organisme peut démontrer que le Parlement l'a autorisé à recueillir les renseignements. Il faudrait donc qu'un texte juridique (loi ou règlement) encadre tout système usant d'une carte à puce, qu'il vise un service à la clientèle ou la prestation d'un programme. Ce texte devrait faire état non seulement des caractéristiques techniques et administratives de la prestation du programme, mais également des codes d'éthique qui régiront la vie privée, la confidentialité et la sécurité.

Les renseignements seront-ils recueillis directement auprès des personnes concernées, et ces dernières seront-elles prévenues des fins de la collecte? Ces deux exigences sont clairement stipulées dans la *Loi sur la protection des renseignements personnels*.

Avis public : le gouvernement devrait, au sens le plus large, prévenir la population des détails entourant la réalisation de tout nouveau système (ses objectifs, sa taille, les renseignements et les clients qu'il vise) avant qu'il n'entre en fonction.

Avis individuel : le gouvernement devrait aviser par écrit chaque détenteur d'une carte à puce des détails entourant son utilisation et la participation au programme qui en fait usage, soient : les fins et la nature du programme, le

cités". La province en a déduit la nécessité d'instaurer des mécanismes de protection de la vie privée avant la conception du réseau. Elle se penchera alors sur la meilleure technologie possible, qui pourrait être la carte à puce.

Cet exemple illustre bien également cette autre tendance (plutôt préoccupante) des gouvernements à se tourner de plus en plus vers le secteur privé pour les aider à assurer leurs services. Des renseignements personnels qui, aujourd'hui encore, sont protégés par une loi dans la plupart des provinces vont être partagés avec des entreprises privées, lesquelles ne sont non seulement assujetties à aucune de ces lois, mais refusent de plus en plus de le devenir, préférant "adhérer" à des codes d'éthique volontaires. Une telle préférence justifie à peine un accès à des renseignements et des transactions qui bénéficient actuellement d'une protection juridique.

Une autre lueur d'espoir brille au Québec, où le gouvernement songe à l'adoption d'une carte à puce dans sa stratégie sur l'autoroute électronique. Comme dans les autres provinces, cette carte à puce à usages multiples remplacerait les autres cartes d'identité québécoises. Mais une différence apparaît au chapitre des usages, alors que le Québec instaurerait cette carte pour l'ensemble de ses programmes, y compris l'octroi de permis de chasse ou de pêche. L'originalité première de la proposition québécoise repose sur trois principes qui doivent guider toute innovation technologique : un accès universel et équitable, le respect de la vie privée et de la confidentialité des renseignements personnels, et le respect des valeurs sociales existantes.

Le projet québécois pourrait bien s'inspirer de l'expérience de carte-santé à puce menée par la province dans la région de Rimouski. Le commissaire québécois à la vie privée, Paul-André Comeau, décrivait dans son rapport du projet que le succès de ce dernier était dû d'abord et avant tout aux assurances offertes par les concepteurs en matière de confidentialité, ainsi qu'au choix d'une technologie apte à soutenir ces assurances. D'après monsieur Comeau, les habitants de Rimouski se sont ralliés au projet lorsque leurs connaissances des garanties de confidentialité ont apaisé leurs craintes. Il a rajouté que le projet avait réussi grâce à l'importante collaboration entre toutes les personnes impliquées dans l'implantation d'une nouvelle technologie pouvant affecter la circulation de renseignements personnels.

Les cartes à puce peuvent détruire notre vie privée. Mais elles peuvent aussi la renforcer. Nous pouvons leur confier un rôle de surveillance et ainsi contrôler notre prochain. Mais nous pouvons aussi les charger de restreindre l'usage et la communication de nos renseignements personnels, de protéger ces derniers, et

demandera un service, il devra insérer sa carte dans un lecteur électronique qui comparera l'empreinte numérisée de la puce à celle de son doigt. L'empreinte numérisée ne peut être entreposée que dans la puce, ce qui en laisse le contrôle au prestataire.

L'envers de la médaille est que le montant des allocations de bien-être social sera versé directement dans la puce de la carte, et que tout achat pourra en être directement débité en magasin : le simple fait d'utiliser cette carte révélera alors que son détenteur est prestataire de bien-être social, ce qui pourrait stigmatiser ce dernier. Un autre impact négatif découle de l'imposition à une partie de la population d'un mécanisme de surveillance habituellement réservé aux criminels et auquel échappe le reste des citoyens. Il est évident que ces cartes à puce ne surveilleront pas les faits et gestes des gens. Une fois le système en marche, toutefois, une simple modification permettrait de recueillir des renseignements reliés au mode de vie et aux habitudes d'achat des prestataires, renseignements qui pourraient aussi intéresser les chercheurs du domaine des sciences sociales. Les cartes à puce devraient permettre, en éliminant les fraudeurs qui touchent plus d'un chèque, d'économiser 32 millions du 1,1 milliard de dollars que coûte annuellement le système de bien-être social.

En Colombie-Britannique, il serait question de regrouper le permis de conduire, la carte d'assurance-maladie et la carte de bien-être social en une seule carte à puce à photographier au laser. David Flaherty, commissaire provincial à la vie privée, considère que cette idée porte atteinte à la vie privée des citoyens, et la *Civil Liberties Association* de la Colombie-Britannique ne se ralliera au concept que si la carte n'est utilisée qu'à des fins d'identification.

Comment gérer une carte-santé à puce?

Les provinces du centre songent également aux cartes à puce comme mécanisme de prestation de services de santé, espérant ainsi réaliser des économies en contrôlant plus strictement les réclamations des citoyens et des professionnels de la santé. Ainsi, le réseau informatique que propose le Manitoba permettrait d'échanger des renseignements médicaux n'importe où dans la province, et d'y accéder à des fins de recherche. Le gouvernement provincial a accordé à la compagnie SmartHealth, filiale de la Banque royale du Canada, un contrat lui demandant d'examiner cette proposition.

L'exemple manitobain démontre la meilleure approche possible : l'examen des besoins avant la recherche d'une solution technologique. Les nombreux groupes de discussion, sondages et entrevues réalisés par SmartHealth ont révélé que "la crainte que des renseignements personnels de nature médicale puissent être vus par des personnes non autorisées revenait fréquemment parmi les préoccupations

De l'éthique et des cartes à puce

Nos rapports annuels traitent régulièrement des cartes d'identité. Cette année encore, le menu est varié. Quantité de suggestions, dont la plupart impliquent l'usage de nouvelles technologies attirantes, découlent de la volonté des gouvernements de réduire leurs dépenses, de simplifier et privatiser la prestation de leurs services et de se débarrasser des fraudeurs.

Ces suggestions reposent souvent sur l'utilisation d'une carte d'identité à usages multiples ou d'une carte à puce ressemblant aux cartes de plastique que l'on retrouve aujourd'hui dans bien des portefeuilles. Mais ces cartes contiennent de puissants circuits et des puces électroniques qui peuvent enregistrer, entreposer et traiter de grandes quantités de renseignements. Ces cartes peuvent, une fois insérées dans des lecteurs électroniques, remplir les fonctions d'un ordinateur branché sur un réseau. Leur popularité vient de leur faible coût, de leur polyvalence, de leur simplicité d'utilisation et de leur puissance. Elles sont devenues une autre de ces nouvelles options qui intriguent tellement les bureaucrates et les gestionnaires du secteur privé qui recherchent, tant pour notre bénéfice que pour leur marge de profit, des façons plus économiques et efficaces d'assurer la prestation de leurs services. Le journaliste John Ibbotson décrit bien la popularité croissante de ces cartes, les qualifiant dans un récent article du *Ottawa Citizen* de "panacée plastifiée".

Mais ces technologies peuvent, si elles sont mal utilisées, devenir de puissants outils de surveillance, signifiant ainsi l'arrêt de mort d'un droit déjà bien faible et menacé. Ceux qui pensent que ces craintes sont exagérées n'ont qu'à se rappeler les fameux propos de ce ministre ontarien commentant l'idée d'une carte à puce à usages multiples pour sa province : cette carte, qui remplacerait le permis de conduite, la carte d'assurance-maladie et celle de bien-être social, et qui surveillerait fidèlement l'usage que les citoyens feraient du système, permettrait "...comme Visa ou Mastercard de dire où vous étiez il y a une heure et ce que vous avez dépensé, ce qui serait une nette amélioration du système de soins de santé en Ontario". Une nette amélioration du point de vue de la gestion du système, peut-être, mais un énorme recul au chapitre de notre autonomie et de notre vie privée.

Carte à puce pour les prestataires de bien-être social

La proposition du conseil municipal de Toronto d'exiger de tous ses prestataires de bien-être social qu'ils aient une carte à puce contenant une de leurs empreintes digitales illustre bien le rôle d'outil de surveillance que peut jouer une telle carte. Cette empreinte digitale n'est plus la version traditionnelle à l'encre, mais en est plutôt une représentation mathématique chiffrée. Chaque fois qu'un prestataire

nous a effectivement amenés à l'ère de l'information, mais nous avons négligé en cours de route nos responsabilités envers notre prochain.

En fait, il est stupéfiant de constater à quel point nous perdons de vue notre dignité d'être humain lorsque nous tentons d'améliorer notre sort. Nous ne devons pas nous contenter de voir la technologie satisfaire nos désirs matériels : si nous ne voulons pas voir notre existence obéir à la technologie, cette dernière doit aussi contribuer à affirmer notre dignité et à réaliser notre potentiel humain.

Chacun a sa part de responsabilité sociale en ce monde électronique. Chacun doit préserver l'équilibre entre un besoin légitime d'information et le respect de son prochain, de ses biens et de ses droits. Contrairement à ce que certains en pensent, nous ne pouvons plus nous permettre d'agir pour la simple raison que la technologie nous le permet. Nous devons désormais étudier les impacts éthiques de la technologie, et contrôler ces derniers dès la conception de nouveaux produits ou services. Nous devons apprendre à nos enfants à respecter dans l'univers électronique les notions de moralité, de civilité, de respect et de communication. En bref, nous devons axer la technologie sur l'éthique.

Tout se résume à une question : à quel point respectons-nous notre prochain, son unicité, ses valeurs personnelles et son droit de les garder secrètes? Pour bien le respecter, nous devons lui reconnaître son droit à une vie privée, et notre liberté s'arrête généralement là où commence sa vie privée. Le juge La Forest, de la Cour Suprême, le résumait bien dans un jugement émis en 1990, lequel caractérisait l'essence d'une société libre comme étant l'absence d'obligation de révéler nos secrets à autrui. L'abandon de notre droit à une vie privée et la perception de notre prochain comme étant un simple numéro à surveiller autant que ses semblables signifient notre abandon de ces valeurs fondamentales et démocratiques que sont nos droits à l'autonomie et de contrôler notre vie. Notre enthousiasme et nos attentes ne serviront à rien si nous nous bornons à mémoriser de nouveaux gestes sans pour autant augmenter notre savoir, notre sagesse et notre respect d'autrui. Bref, nous devons ériger une solide infrastructure éthique à l'univers technologique.

Ne mêlons pas nos mots : quelle que soit la quantité de renseignements ou de technologies à notre disposition, nous n'en tirerons aucun profit si leur valeur nous est inconnue.

John Naisbitt

Monsieur Manley et son homologue de la Justice se sont engagés à consulter les provinces et "les autres intervenants" afin de proposer "une loi-cadre régissant la protection des renseignements personnels dans le secteur privé". Va-t-on enfin voir un geste significatif?

Rien ne permettrait de mieux contrer les risques que la révolution technologique fait courir à notre vie privée que l'imposition de paramètres d'ordre, d'équité et de respect aux pratiques qu'adoptent les entreprises privées pour la gestion de leurs renseignements. Après tout, ces entreprises sont celles qui recueillent et utilisent le plus de renseignements de leurs clients et de leurs employés, tout en reconnaissant et en respectant le moins leurs droits.

Monsieur Manley n'est évidemment pas rentré dans les détails, puisque son projet n'en est qu'à ses débuts. Mais ces détails sont généralement là où surgissent les difficultés. Le gouvernement a donc le choix : promouvoir une loi réellement efficace qui verra enfin la technologie respecter de façon civilisée les droits de l'être humain, trop hésiter, ou permettre comme à l'habitude que son élan initial soit freiné par des intérêts particuliers. Dans ces deux derniers cas, nous hériterons d'un ramassis de dispositions sectorielles inefficaces qui permettront davantage de surveiller nos moindres mouvements que de nous rendre le contrôle des renseignements que nous disséminons. Il vaudrait alors mieux n'avoir aucune loi, évitant ainsi de nous leurrer.

Notre population est arrivée à un point critique de son histoire, alors qu'elle doit décider de sauver ou d'abandonner ce qui lui reste de vie privée. Son sort dépend maintenant de la volonté et de l'initiative de ses élus.

Et si nous respectons notre prochain?

Nous avons effectivement besoin de meilleures lois pour protéger notre vie privée. Mais ces lois ne suffisent pas, car leurs mots ne représentent qu'un consensus stipulant les principes éthiques fondamentaux entourant les actes et les interdits à la base de nos valeurs sociales et de notre conduite individuelle ou collective. Ces mots ne prendront vie que si nous partageons de grands principes éthiques qui nous soudent. Il est maintenant temps de bien évaluer les enjeux éthiques découlant des nouvelles technologies.

La presse écrite ne cesse de nous prouver à quel point nous nous désolidarisons les uns des autres. À preuve, ces pirates informatiques qui s'introduisent de force dans les ordinateurs pour en lire ou en détruire les données, à moins qu'ils ne décident de vous jouer un tour ou de vous harceler électroniquement, ou encore de diffuser leurs messages haineux, violents ou pornographiques. La technologie

gouvernement ait publiquement reconnu qu'une telle clause n'aurait en rien diminué les chances de privatiser le système de navigation aérienne...

Les responsables de NAVCANADA se sont quant à eux engagés à obtenir de chaque employé l'autorisation que son dossier fédéral leur soit transféré, ainsi qu'à en garantir la confidentialité "aux termes de la politique fédérale". De beaux engagements, certes, mais sans valeur juridique, et bien moindres que la protection dont bénéficiaient ces employés. Le Commissariat prévoit inspecter les dossiers de ces derniers avant que Transport Canada ne s'en départisse.

Le système canadien de navigation aérienne est le premier de plusieurs programmes que le gouvernement fédéral a l'intention de privatiser. Devrait ensuite disparaître le Groupe communication Canada, énorme organisme chargé de l'impression et de la diffusion des documents du gouvernement, ainsi que de ses services de renseignements. Bien des ports et des aéroports ont déjà été vendus, et de nouvelles "agences de services" vont bientôt faire leur apparition, lesquelles assumeront certaines activités actuellement assurées par des organismes fédéraux : Parcs Canada (anciennement du ministère de l'Environnement), Agro-alimentaire Canada (nouvelle agence d'inspections alimentaires), et la Commission canadienne sur le revenu (découlant de Revenu Canada). Ces nouvelles agences auront une plus grande latitude que le gouvernement fédéral, ce qui leur permettra d'améliorer leurs services, de réduire leurs coûts de fonctionnement et de mieux impliquer les provinces. Mais tous ces mécanismes plus souples, ces services améliorés et les nouvelles lois les habilitant vont-ils signifier la disparition du droit à la vie privée des clients et des employés affectés?

Le tunnel a-t-il une fin?

Un vague espoir semble naître de la réponse fédérale aux recommandations du Conseil consultatif sur l'autoroute électronique. Se faisant quelque peu désirer, le ministre de l'Industrie vient enfin d'annoncer que le gouvernement mettrait en place une loi obligeant les entreprises privées à respecter la vie privée de leurs employés et de leurs clients. Cette déclaration de John Manley est la plus importante que nous ayons entendue ces dernières années, sinon même la plus importante de toute l'histoire canadienne de la protection de la vie privée.

Le gouvernement fédéral, dans son rapport intitulé *Pour entrer de plain-pied dans le XXI^e siècle*, "reconnait que, comme on ne peut pas uniquement compter sur la technologie et les mesures de sécurité, le droit à la protection des renseignements personnels doit être reconnu dans la loi, surtout dans un monde électronique de bases de données privées où il est très facile de recueillir et d'exploiter des renseignements sur une personne".

La meilleure illustration de ce désastre reste le transfert du système de navigation aérienne et de près de 6 000 fonctionnaires fédéraux à NAVCANADA, une entreprise privée, sans parler de la grande quantité de renseignements personnels découlant des opérations de contrôle de la navigation aérienne et provenant des milliers d'utilisateurs de ce système.

Un transfert d'une telle importance ne pouvait rester sous silence, et le Commissaire a écrit au gouvernement en novembre dernier pour lui en décrire les conséquences pour la vie privée. Sa lettre comportait également une solution : le gouvernement pouvait, dans son contrat le liant à NAVCANADA, assujettir cette dernière à la *Loi sur la protection des renseignements personnels* tout aussi facilement qu'il l'avait déjà assujettie à la *Loi sur les langues officielles*.

La suggestion du Commissaire est cependant restée lettre morte, bien que le gouvernement ait reconnu l'importance de l'enjeu. Le Commissaire a alors comparu devant le Comité des transports de la Chambre des Communes qui étudiait le projet de transfert. Ses membres ont accepté sa suggestion et l'ont recommandée au reste des députés fédéraux. Mais suite à un second rejet de la part du gouvernement, et malgré une troisième tentative du Commissaire auprès du Comité sénatorial, le projet de loi a été adopté par les deux Chambres sans contenir aucune mesure de protection de la vie privée.

Les objections du gouvernement et de NAVCANADA portaient surtout sur le fait que la suggestion du Commissaire aurait imposé à cette compagnie un fardeau auquel échappe le reste des entreprises privées, libres de toute réglementation quant au respect de la vie privée. Rien n'est cependant plus faux.

Le gouvernement fédéral oblige déjà ses organismes à incorporer aux contrats les liants à des entreprises privées des clauses assujettissant ces dernières aux dispositions pertinentes de la *Loi sur la protection des renseignements personnels*. Et que dire de la Société canadienne des postes, dont la gigantesque opération est restée sujette à la Loi même après la refonte en profondeur de sa structure corporative vers une entreprise commerciale quasi privée? Même si elle reste la propriété du gouvernement fédéral, la SCP doit subir une concurrence farouche du secteur privé dans la poursuite de ses activités. Le monopole qu'est NAVCANADA, lui, ne connaîtra jamais les angoisses d'une telle concurrence.

Quel que soit le sort réservé à tous ces arguments, le gouvernement devrait être obligé, lors de chaque privatisation, de préserver nos droits à notre vie privée et à la protection de nos renseignements personnels. Et y a-t-il façon plus facile de s'acquiescer de cette obligation que de rajouter une simple clause à un contrat ou un projet de loi? Surtout après que l'un des principaux négociateurs du

À quel saint se vouer?

"La liberté individuelle doit céder le pas à la nécessité. Ainsi pensent le tyran et l'esclave." — William Pitt, dit le Second, 1793.

Ces paroles, prononcées il y a plus de deux siècles par un grand homme politique britannique, étaient tout aussi pertinentes et ponctuelles qu'elles le sont aujourd'hui, alors que nous luttons pour préserver le reste de notre vie privée. Il ne se passe pas une journée sans que notre société, déjà emportée par un tourbillon de nouvelles technologies, ne soit assaillie par des arguments prétendant la nécessité d'une nouvelle atteinte à notre vie privée. Et quels arguments! Ces irréversibles bénéfices (réels, hypothétiques ou illusoire) que sont l'efficacité, la commodité et les économies profitent à ceux qui ont tout à y gagner.

Le tyran de ces lignes n'est pas un dictateur militaire, mais plutôt notre ignorance, qui nous pousse à adopter sans hésitation toutes ces nouvelles technologies sans penser à leurs conséquences. Dans notre cas, nous sommes et le tyran et l'esclave.

Un dangereux recul

La lutte paraissait pourtant gagnée au sein du gouvernement fédéral. Mais les derniers mois nous ont sérieusement malmenés, alors que des milliers de Canadiens ont perdu leur droit au respect de leur vie privée suite à la refonte et à la privatisation d'organismes fédéraux. Les innombrables renseignements que détenaient ces organismes vont maintenant passer sous le contrôle d'entreprises privées, perdant ainsi la protection dont ils jouissaient en vertu de la *Loi sur la protection des renseignements personnels*, et dont les pratiques équitables de gestion de l'information ne les régiront plus : en effet, les personnes visées par ces renseignements ne pourront plus légalement en prendre connaissance ni en contrôler la collecte, l'usage, la communication ou la destruction.

La vente de l'appareil fédéral affecte plus visiblement les milliers de fonctionnaires qui passent à l'emploi du secteur privé. Mais elle a également un impact sur les innombrables Canadiens qui recourent aux services qu'assuraient ces fonctionnaires.

L'état de notre vie privée est désormais désastreux, et la réputation du gouvernement canadien à ce chapitre, auparavant enviable, est maintenant entachée. Ce regrettable effet de la privatisation, peut-être purement involontaire, aurait cependant pu être évité car il est impensable qu'il n'ait pas été prévu.

Table des matières

À quel saint se vouer? 1

De l'éthique et des cartes à puce 6

Naissance d'une base de données génétiques 13

Voter librement? 15

Le grand partage 18

Parlons de télécommunications 22

Silence ou publicité? 25

Le système de gestion des casiers judiciaires 28

Internet et vie privée : guide de l'utilisateur 30

L'Institut canadien d'information sur la santé 33

Des lois protégeant la vie privée 35

Enquêtes 36

 Demandes de renseignements 44

 Tableaux 46

Observation de la loi 51

 Vérifications 56

 Suivis 61

 Etude sur le partage de renseignements 62

Aperçu juridique 67

Le rôle de missionnaire des Affaires publiques 68

Direction de la gestion intégrée 70

Organigramme 72

- 20h20 **Commande de vêtements par catalogue** (la compagnie enregistre tous les détails de la commande et votre numéro de carte de crédit, et peut les vendre à des entreprises de vente de listes nominatives)
- 20h30 **Abonnement à une nouvelle revue** (la majorité des éditeurs de revue vendent leur liste d'abonnés à des compagnies de publipostage)
- 20h35 **Appel téléphonique d'une maison de sondage** (ces compagnies s'intéressent à vos opinions politiques, à vos goûts personnels et à vos habitudes de vie; certains sondages sont en fait des campagnes de publicité permettant à des compagnies de recruter vos renseignements personnels en vue de promotions ultérieures; les véritables maisons de sondage détruisent vos renseignements personnels une fois que les données ont été compilées)
- 20h45 **Visite d'un prospecteur d'un parti politique** (tout don à un parti politique d'un montant supérieur à 100\$ devient un renseignement disponible au public)
- 21h10 **Ouverture de session Internet** (les groupes de discussion auxquels vous participez ainsi que le contenu de vos messages peuvent être surveillés, et n'importe qui, y compris la police, peut établir un profil de qui vous êtes; beaucoup de sites Web enregistrent vos visites; voir aussi *Internet et vie privée* en page 30)

Comme vous voyez, il semble bien que la vie dans les villes d'aujourd'hui ne nous laisse plus beaucoup d'endroits ni de moments pour nous cacher. Notre quête d'une sécurité accrue et d'un plus grand confort est-elle en fait en train de nous asservir à l'électronique et à l'informatique?

Faits saillants de ce rapport

- La vie privée des Canadiens est affaiblie par la vente sans conditions des programmes fédéraux au secteur privé (page 1);
- Une nouvelle liste électorale permanente se prépare : quelles erreurs éviter ? (page 15);
- Les criminels dangereux dans nos villes : faut-il vraiment le savoir ? (page 25);
- La vie privée et l'univers électronique : conseils pour les internautes (page 30);
- Un cadre de référence pour l'usage de cartes à puce polyvalentes (page 6);
- 1681 plaintes de réglées, et des réponses à plus de 9000 demandes de renseignements (page 36).

- 12h35 **Rendez-vous chez le médecin** (les cartes d'assurance-maladie auront bientôt une puce informatique qui entreposera tout votre dossier médical; l'ADN de votre échantillon de sang pourrait être testé afin de détecter n'importe quelle maladie ou prédisposition; le diagnostic de votre docteur pourra être divulgué à la compagnie d'assurances à laquelle vous avez demandé une police d'assurance-vie ou invalidité, et un résumé de ce diagnostic sera peut-être acheminé à un registre central que les compagnies d'assurance financent aux États-Unis)
- 13h15 **Achat de médicaments** (certaines provinces ont relié leurs pharmacies par ordinateur, lesquelles ont toutes accès à votre dossier pharmaceutique; certains corps policiers chargés de l'enquête d'abus de médicaments ou de drogues peuvent aussi y avoir accès)
- 13h30 **Retour au bureau** (la carte prend note de votre retour)
- 14h45 **Fourniture d'un échantillon d'urine à votre employeur dans le cadre de son programme de dépistage anti-drogue** (les résultats du test révéleront l'usage de certaines drogues, mais n'indiqueront pas si vous êtes en état de travailler; ces résultats pourront aussi indiquer la présence de médicaments autorisés, tels les pilules anticonceptionnelles, l'insuline et les antidépresseurs)
- 15h30 **Réunion dans un local sous haute sécurité** (vous devez passer par la barrière de sécurité, où une machine lit les motifs de votre rétine pour confirmer votre identité)
- 17h30 **Rédaction de la première ébauche de votre rapport** (votre ordinateur entrepose le contenu de ce rapport, mais peut aussi mesurer votre vitesse de frappe, votre taux d'erreur, la longueur des pauses que vous prenez et celle de vos absences)
- 18h15 **Départ de votre bureau** (ce départ est enregistré par votre ordinateur, le système d'accès et le stationnement)
- 18h30 **Courses** (le fait que vous payez par carte de débit est enregistré, et la carte-loyauté de l'épicerie mémorise vos achats à des fins de publicité et de rabais ciblés)
- 18h45 **Location d'un film vidéo** (l'ordinateur de votre club enregistre votre numéro d'assurance-sociale, le titre de tous les films que vous avez loués, et peut vendre cette liste de titres (de films pornographiques?) à d'autres compagnies)
- 19h20 **Écoute de vos messages téléphoniques** (votre système téléphonique a enregistré le numéro de téléphone des personnes qui vous ont appelé, et il divulgue le vôtre à vos interlocuteurs à moins que vous ne l'en empêchiez en composant un code)

peut étudier les tendances que révèlent vos dépenses pour élaborer avec précision votre profil)

Une journée typique de votre vie... vue par les ordinateurs

Alors, vous n'avez rien à cacher, il paraît? Tant mieux! Car du moment où vous vous réveillez à celui où vous endormez, vos moindres gestes sont notés, analysés, documents et même commercialisés, et tout cela sans votre autorisation ni même que vous le sachiez! Et il n'y a rien d'illégal à tout cela (sauf au Québec).

- 8h30 Sortie du stationnement de votre immeuble (cette sortie est filmée par caméra et peut-être même inscrite sur une carte)
- 8h35 Entrée sur l'autoroute à péage (votre entrée, ainsi que votre sortie de cette autoroute, est notée par des machines programmées pour vous envoyer une facture mensuelle)
- 8h42 Bouchon de circulation, appel à votre bureau pour retarder une réunion (les appels faits sur téléphone cellulaire peuvent facilement être interceptés; les nouveaux téléphones personnels indiqueront à tout moment votre emplacement aux satellites chargés de vous transmettre vos appels)
- 9h17 Entrée dans le stationnement de votre bureau (une carte enregistre la date et l'heure, et une caméra surveille le stationnement)
- 9h20 Entrée par la porte principale de votre bureau ou usine (une carte à bande magnétique enregistre vos déplacements, et votre badge électronique permet de vous retrouver en tout temps dans le bâtiment)
- 9h25 Ouverture de session à votre ordinateur (le système informatique enregistre l'heure)
- 9h29 Envoi d'un message électronique personnel à un ami, et d'un second message, professionnel, à un collègue (les deux messages peuvent être lus par votre employeur, même si vous les effacez de votre écran : ils restent sur le disque rigide de l'ordinateur central)
- 10h45 Appel à votre mère (votre superviseur écoute peut-être vos appels)
- 11h00 Livraison au volant d'une voiture de votre compagnie (ces voitures ont généralement un émetteur en permettant la localisation et son affichage, certaines sont même équipées d'une "boîte noire" mémorisant les habitudes de conduite des gens)
- 12h05 Arrêt au guichet bancaire automatisé (le système enregistre les détails de la transaction, et une caméra, installée soit dans le guichet ou au-dessus, filme vos gestes)
- 12h10 Achat d'un cadeau pour l'anniversaire d'une amie (le lecteur de la carte de crédit enregistre les détails de votre transaction, la carte-loyauté du magasin assigne des points et des rabais ciblés à votre achat, votre banque



Commissaire
à la protection de
la vie privée du Canada

Privacy
Commissioner
of Canada

L'honorable Gilbert Parent
Président
Chambre des communes
Ottawa

juillet 1996

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Le rapport couvre la période allant du 1^{er} avril 1995 au 31 mars 1996.

Veillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire,

Bruce Phillips

Bruce Phillips



Commissaire
à la protection de
la vie privée du Canada

Privacy
Commissioner
of Canada

L'honorable Gildas L. Molgat
Président
Sénat
Ottawa

juillet 1996

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Le rapport couvre la période allant du 1^{er} avril 1995 au 31 mars 1996.

Veuillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le commissaire,

Bruce Phillips

Bruce Phillips

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-2410, 1-800-267-0441
Téléc. (613) 947-6850
ATS (613) 992-9190

© Groupe communication Canada
N° de cat. 30-1/1996
ISBN 0-662-62582-X

Cette publication est offerte sur cassette et sur disquette informatique. Nous sommes accessibles sur le réseau Internet à : <http://infoweb.magi.com/~privcan/>

Rapport annuel du
Commissaire à la protection
de la vie privée
1995-1996





Commissaire à la protection de la vie privée

M1

A P P O R T A N N U E L

